

PATENT COOPERATION TREATY

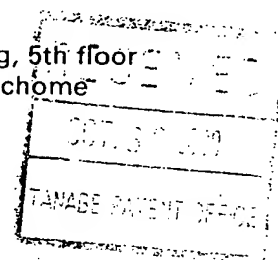
PCT

NOTICE INFORMING THE APPLICANT OF THE
COMMUNICATION OF THE INTERNATIONAL
APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

From the INTERNATIONAL BUREAU

To:

TANABE, Shigemoto
Green-Fantasia Building, 5th floor
11-11-508, Jingumae 1-chome
Shibuya-ku
Tokyo 150-0001
JAPON

Date of mailing (day/month/year) 19 October 2000 (19.10.00)		
Applicant's or agent's file reference S00P0778WO00		IMPORTANT NOTICE
International application No. PCT/JP00/02289	International filing date (day/month/year) 07 April 2000 (07.04.00)	
		Priority date (day/month/year) 12 April 1999 (12.04.99)
Applicant SONY CORPORATION et al		

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
KR,US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
CN,EP,SG

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on 19 October 2000 (19.10.00) under No. WO 00/62216.

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer J. Zahra Telephone No. (41-22) 338.83.38
--	---

Attorney Docket No. 450108-02550

New Patent Application filed **December 8, 2000**, entitled:

**INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING
METHOD, AND PROVIDING MEDIUM**

corresponding to PCT Application No. PCT/JP00/02289

filed April 7, 2000

Express Mail No.: EL585030619US

Date of Deposit: December 8, 2000


I hereby certify that this application and the accompanying papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Box PCT
Assistant Commissioner for Patents
Washington, D.C. 20231.



特 許 協 力 条 約

発信人 日本国特許庁（国際調査機関）

出願人代理人	
田辺 恵基	
あて名	
〒150-0001	
東京都渋谷区神宮前1丁目11番11-508号 グリーンファンタジアビル5階 田辺特許事務所	

殿

PCT

国際調査報告又は国際調査報告を作成しない旨
の決定の送付の通知書

（法施行規則第41条）
〔PCT規則44.1〕

発送日 (日.月.年) 13.06.00	今後の手続きについては、下記1及び4を参照。
国際出願番号 PCT/JP00/02289	国際出願日 (日.月.年) 07.04.00
出願人（氏名又は名称） ソニー株式会社	

1. <input checked="" type="checkbox"/> 国際調査報告が作成されたこと、及びこの送付書とともに送付することを、出願人に通知する。 PCT19条の規定に基づく補正書及び説明書の提出 出願人は、国際出願の請求の範囲を補正することができる（PCT規則46参照）。 いつ 補正書の提出期間は、通常国際調査報告の送付の日から2月である。 詳細については添付用紙の備考を参照すること。 どこへ 直接次の場所へ The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22)740.14.35 詳細な手続については、添付用紙の備考を参照すること。
2. <input type="checkbox"/> 国際調査報告が作成されないこと、及び法第8条第2項（PCT17条(2)(a)）の規定による国際調査報告を作成しない旨の決定をこの送付書とともに送付することを、出願人に通知する。
3. <input type="checkbox"/> 法施行規則第44条（PCT規則40.2）に規定する追加手数料の納付に対する異議の申立てに関して、出願人に下記の点を通知する。 <input type="checkbox"/> 異議の申立てと当該異議についての決定を、その異議の申し立てと当該異議についての決定の両方を指定官庁へ送付することを求める出願人の請求とともに、国際事務局へ送付した。 <input type="checkbox"/> 当該異議についての決定は、まだ行われていない。決定されしだい出願人に通知する。
4. 今後の手続： 出願人は次の点に注意すること。 優先日から18月経過後、国際出願は国際事務局によりすみやかに国際公開される。出願人が公開の延期を望むときは、国際出願又は優先権の主張の取下げの通知がPCT規則90の2.1及び90の2.3にそれぞれ規定されているように、国際公開の事務的な準備が完了する前に国際事務局に到達しなければならない。 出願人が優先日から30月まで（官庁によってはもっと遅く）国内段階の開始を延期することを望むときは、優先日から19月以内に、国際予備審査の請求書が提出されなければならない。 国際予備審査の請求書若しくは、後にする選択により優先日から19箇月以内に選択しなかった又は第II章に拘束されないため選択できなかったすべての指定官庁に対しては優先日から20月以内に、国内段階の開始のための所定手続を取らなければならない。

名称及びあて名 日本国特許庁（ISA/JP） 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	権限のある職員 特 許 庁 長 官 電話番号 03-3581-1101 内線 3562	5 L 9 2 8 7
--	---	-------------

注 意

1. 国際調査報告の発送日から起算する条約第19条(1)及び規則46.1に従う国際事務局への補正期間に注意してください。
2. 条約22条(2)に規定する期間に注意してください。
3. 文献の写しの請求について

国際調査報告に記載した文献の複写

特許庁にこれらの引用文献の写しを請求することもできますが、日本特許情報機構でもこれらの引用文献の複写物を販売しています。日本特許情報機構に引用文献の複写物を請求する場合は下記の点に注意してください。

〔申込方法〕

- (1) 特許(実用新案・意匠)公報については、下記の点を明記してください。

○特許・実用新案及び意匠の種類

○出願公告又は出願公開の年次及び番号(又は特許番号、登録番号)

○必要部数

- (2) 公報以外の文献の場合は、下記の点に注意してください。

○国際調査報告の写しを添付してください(返却します)。

〔申込み及び照会先〕

〒135 東京都江東区東陽4-1-7 佐藤ダイヤビル

財団法人 日本特許情報機構 サービス課

TEL 03-5690-3900

注意 特許庁に対して文献の写しの請求をすることができる期間は、国際出願日から7年です。

様式PCT/ISA/220の備考

この備考は、PCT 19条の規定に基づく補正書の提出に関する基本的な指示を与えるためのものである。この備考は特許協力条約並びにこの条約に基づく規則及び実施細則の規定に基づいている。この備考とそれらの規定とが相違する場合には、後者が適用される。詳細な情報については、WIPOの出版物であるPCT出願人の手引も参照すること。

PCT 19条の規定に基づく補正書の提出に関する指示

出願人は、国際調査報告を受領した後、国際出願の請求の範囲を補正する機会が一回ある。しかし、国際出願のすべての部分（請求の範囲、明細書及び図面）が、国際予備審査の手続においても補正できるもので、例えば出願人が仮保護のために補正書を公開することを希望する場合又は国際公開前に請求の範囲を補正する別の理由がある場合を除き、通常PCT 19条の規定に基づく補正書を提出する必要はないことを強調しておく。さらに、仮保護は一部の国のみで与えられるだけであることも強調しておく。

補正の対象となるもの

PCT 19条の規定により請求の範囲のみ補正することができる。

国際段階においてPCT 34条の規定に基づく国際予備審査の手続において請求の範囲を（更に）補正することができる。

明細書及び図面は、PCT 34条の規定に基づく国際予備審査の手続においてのみ補正することができる。

国内段階に移行する際、PCT 28条（又はPCT 41条）の規定により、国際出願のすべての部分を補正することができる。

いつ

国際調査報告の送付の日から2月又は優先日から16月の内どちらか遅く満了するほうの期間内。しかし、その期間の満了後であっても国際公開の技術的な準備の完了前に国際事務局が補正を受領した場合には、その補正書は、期間内に受理されたものとみなすことを強調しておく（PCT規則46.1）。

補正書を提出すべきところ

補正書は、国際事務局のみに提出でき、受理官庁又は国際調査機関には提出してはいけない（PCT規則46.2）。国際予備審査の請求書を提出した／する場合については、以下を参照すること。

どのように

1以上の請求の範囲の削除、1以上の新たな請求の範囲の追加、又は1以上の請求の範囲の記載の補正による。

差替え用紙は、補正の結果、出願当初の用紙と相違する請求の範囲の各用紙毎に提出する。

差替え用紙に記載されているすべての請求の範囲には、アラビア数字を付さなければならない。請求の範囲を削除する場合、その他の請求の範囲の番号を付け直す必要はない。請求の範囲の番号を付け直す場合には、連続番号で付け直さなければならない（PCT実施細則第205号(b)）。

補正は国際公開の言語で行う。

補正書にどのような書類を添付しなければならないか

書簡（PCT実施細則第205号(b)）

補正書には書簡を添付しなければならない。

書簡は国際出願及び補正された請求の範囲とともに公開されることはない。これを「PCT 19条(1)に規定する説明書」と混同してはならない（「PCT 19条(1)に規定する説明書」については、以下を参照）。

書簡は、英語又は仏語を選択しなければならない。ただし、国際出願の言語が英語の場合、書簡は英語で、仏語の場合、書簡は仏語で記載しなければならない。

書簡には、出願時の請求の範囲と補正された請求の範囲との相違について表示しなければならない。特に、国際出願に記載した各請求の範囲との関連で次の表示（2以上の請求の範囲についての同一の表示する場合は、まとめることができる。）をしなければならない。

- (i) この請求の範囲は変更しない。
- (ii) この請求の範囲は削除する。
- (iii) この請求の範囲は追加である。
- (iv) この請求の範囲は出願時の1以上の請求の範囲と差し替える。
- (v) この請求の範囲は出願時の請求の範囲の分割の結果である。

次に、添付する書簡中での、補正についての説明の例を示す。

1. [請求の範囲の一部の補正によって請求の範囲の項数が48から51になった場合] :
“請求の範囲1-29、31、32、34、35、37-48項は、同じ番号のもとに補正された請求の範囲と置き換えられた。請求の範囲30、33及び36項は変更なし。新たに請求の範囲49-51項が追加された。”
2. [請求の範囲の全部の補正によって請求の範囲の項数が15から11になった場合] :
“請求の範囲1-15項は、補正された請求の範囲1-11項に置き換えられた。”
3. [原請求の範囲の項数が14で、補正が一部の請求の範囲の削除と新たな請求の範囲の追加を含む場合] :
“請求の範囲1-6及び14項は変更なし。請求の範囲7-13は削除。新たに請求の範囲15、16及び17項を追加。” 又は
“請求の範囲7-13は削除。新たに請求の範囲15、16及び17項を追加。その他の全ての請求の範囲は変更なし。”
4. [各種の補正がある場合] :
“請求の範囲1-10項は変更なし。請求の範囲11-13、18及び19項は削除。請求の範囲14、15及び16項は補正された請求の範囲14項に置き換えられた。請求の範囲17項は補正された請求の範囲15、16及び17項に分割された。新たに請求の範囲20及び21項が追加された。”

“PCT19条(1)の規定に基づく説明書”(PCT規則46.4)

補正書には、補正並びにその補正が明細書及び図面に与える影響についての説明書を提出することができる(明細書及び図面はPCT19条(1)の規定に基づいては補正できない)。

説明書は、国際出願及び補正された請求の範囲とともに公開される。

説明書は、国際公開の言語で作成しなければならない。

説明書は、簡潔でなければならない、英語の場合又は英語に翻訳した場合に500語を越えてはならない。

説明書は、出願時の請求の範囲と補正された請求の範囲との相違を示す書簡と混同してはならない。説明書を、その書簡に代えることはできない。説明書は別紙で提出しなければならない、見出しを付すものとし、その見出しは“PCT19条(1)の規定に基づく説明書”の語句を用いることが望ましい。

説明書には、国際調査報告又は国際調査報告に列記された文献との関連性に関して、これらを誹謗する意見を記載してはならない。国際調査報告に列記された特定の請求の範囲に関連する文献についての言及は、当該請求の範囲の補正に関してのみ行うことができる。

国際予備審査の請求書が提出されている場合

PCT19条の規定に基づく補正書及び添付する説明書の提出の時に国際予備審査の請求書が既に提出されている場合には、出願人は、補正書(及び説明書)を国際事務局に提出すると同時にその写し及び必要な場合、その翻訳文を国際予備審査機関にも提出することが望ましい(PCT規則55.3(a)、62.2の第1文を参照)。詳細は国際予備審査請求書(PCT/IPEA/401)の注意書参照。

国内段階に移行するための国際出願の翻訳に関して

国内段階に移行する際、PCT19条の規定に基づいて補正された請求の範囲の翻訳を出願時の請求の範囲の翻訳の代わりに又は追加して、指定官庁/選択官庁に提出しなければならないこともあるので、出願人は注意されたい。

指定官庁/選択官庁の詳細な要求については、PCT出願人の手引きの第II巻を参照。

PCT

国際調査報告

(法8条、法施行規則第40、41条)
[PCT18条、PCT規則43、44]

出願人又は代理人 の書類記号 S00P0778WO00	今後の手続きについては、国際調査報告の送付通知様式(PCT/ISA/220) 及び下記5を参照すること。	
国際出願番号 PCT/JPO0/02289	国際出願日 (日.月.年) 07.04.00	優先日 (日.月.年) 12.04.99
出願人(氏名又は名称) ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条(PCT18条)の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 2 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

1. 国際調査報告の基礎

a. 言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。

☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

b. この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。

☐ この国際出願に含まれる書面による配列表

☐ この国際出願と共に提出されたフレキシブルディスクによる配列表

☐ 出願後に、この国際調査機関に提出された書面による配列表

☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表

☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。

☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記載した配列が同一である旨の陳述書の提出があった。

2. ☐ 請求の範囲の一部の調査ができない(第I欄参照)。

3. ☐ 発明の単一性が欠如している(第II欄参照)。

4. 発明の名称は ☒ 出願人が提出したものを承認する。

☐ 次に示すように国際調査機関が作成した。

5. 要約は ☒ 出願人が提出したものを承認する。

☐ 第III欄に示されているように、法施行規則第47条(PCT規則38.2(b))の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から1カ月以内にこの国際調査機関に意見を提出することができる。

6. 要約書とともに公表される図は、

第 20 図とする。 ☒ 出願人が示したとおりである。

☐ なし

☐ 出願人は図を示さなかった。

☐ 本図は発明の特徴を一層よく表している。

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年

日本国公開実用新案公報 1971-2000年

日本国実用新案登録公報 1996-2000年

日本国登録実用新案公報 1994-2000年

国際調査で使用了電子データベース (データベースの名称、調査に使用した用語)

JICSTデータベース (JOIS)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO, 96/27155, A2 (InerTrust Technologies Corp.), 6. 9月. 1996 (06. 09. 96&JP, 10-512074, A	1-9
A	US, 6002771, A (Sun Microsystems, Incorporated) 22. 5月. 96 (22. 05. 96)&JP, 10-055383, A	1-9

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

24. 05. 00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

岩間 直純



5L

9287

電話番号 03-3581-1101 内線 3532

特許協力条約に基づく国際出願

願 書

出願人は、この国際出願が特許協力条約に従って処理されることを請求する。

国際出願番号 受理官庁記入欄

国際出願日

(受付印)

出願人又は代理人の書類記号
(希望する場合、最大12字)

S 00 P 0778 W O 00



控

第 I 欄 発明の名称

情報処理装置および方法、並びに提供媒体

PTA/PCT Rec'd 08 DEC 2000

第 II 欄 出願人

氏名 (名称) 及びあて名: (姓・名の順に記載; 法人は公式の完全な名称を記載; あて名は郵便番号及び国名も記載)

ソニー株式会社

SONY CORPORATION

〒141-0001 日本国東京都品川区北品川 6 丁目 7 番 3 5 号

7-35, Kitashinagawa 6-chome, Shinagawa-ku, TOKYO 141-0001, JAPAN

☐ この欄に記載した者は、
発明者でもある。

電話番号:

03-5448-2617

ファクシミリ番号:

03-5448-3063

加入電話番号:

J22262

国籍 (国名): 日本国 JAPAN

住所 (国名): 日本国 JAPAN

この欄に記載した者は、次の

指定国についての出願人である:

☐ すべての指定国

☒ 米国を除くすべての指定国

☐ 米国のみ

☐ 追記欄に記載した指定国

第 III 欄 その他の出願人又は発明者

氏名 (名称) 及びあて名: (姓・名の順に記載; 法人は公式の完全な名称を記載; あて名は郵便番号及び国名も記載)

石橋 義人

ISHIBASHI Yoshihito

〒141-0001 日本国東京都品川区北品川 6 丁目 7 番 3 5 号

ソニー株式会社内

C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, TOKYO 141-0001, JAPAN

この欄に記載した者は
次に該当する:

☐ 出願人のみである。

☒ 出願人及び発明者である。

☐ 発明者のみである。
(ここにレ印を付したとき
は、以下に記入しないこと)

国籍 (国名): 日本国 JAPAN

住所 (国名): 日本国 JAPAN

この欄に記載した者は、次の

指定国についての出願人である:

☐ すべての指定国

☐ 米国を除くすべての指定国

☒ 米国のみ

☐ 追記欄に記載した指定国

☒ その他の出願人又は発明者が続葉に記載されている。

第 IV 欄 代理人又は共通の代表者、通知のあて名

次に記載された者は、国際機関において出願人のために行動する:

☒ 代理人

☐ 共通の代表者

氏名 (名称) 及びあて名: (姓・名の順に記載; 法人は公式の完全な名称を記載; あて名は郵便番号及び国名も記載)

8274 弁理士 田 辺 恵 基

TANABE Shigemoto

〒150-0001 日本国東京都渋谷区神宮前1丁目11番11-508号
グリーンファンタジアビル5階

Green-Fantasia Building 5th Floor, 11-11-508,
Jingumae 1-chome, Shibuya-ku, TOKYO 150-0001, JAPAN

電話番号:

03-3470-6591

ファクシミリ番号:

03-3470-6506

加入電話番号:

☐ 通知のためのあて名: 代理人又は共通の代表者が選任されておらず、上記枠内に特に通知が送付されるあて名を記載している場合は、レ印を付す。

第III欄の続き その他出願人又は発明者

この縦罫を使用しないときは、この用紙を願書に含めないこと。

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

大石 丈於 OHISHI Tateo

〒141-0001 日本国東京都品川区北品川6丁目7番35号

ソニー株式会社内

C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, TOKYO 141-0001, JAPANこの欄に記載した者は、
次に該当する:

- ☐ 出願人のみである。
- ☒ 出願人及び発明者である。
- ☐ 発明者のみである。
(ここにレ印を付したときは、以下に記入しないこと)

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の

指定国についての出願人である:

- ☐ すべての指定国 ☐ 米国を除くすべての指定国 ☒ 米国のみ ☐ 追記欄に記載した指定国

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

武藤 明宏 MUTO Akihiro

〒141-0001 日本国東京都品川区北品川6丁目7番35号

ソニー株式会社内

C/O SONY CORPORATION, 7-35, Kitashinagawa 6-chome,
Shinagawa-ku, TOKYO 141-0001, JAPANこの欄に記載した者は、
次に該当する:

- ☐ 出願人のみである。
- ☒ 出願人及び発明者である。
- ☐ 発明者のみである。
(ここにレ印を付したときは、以下に記入しないこと)

国籍(国名): 日本国 JAPAN

住所(国名): 日本国 JAPAN

この欄に記載した者は、次の

指定国についての出願人である:

- ☐ すべての指定国 ☐ 米国を除くすべての指定国 ☒ 米国のみ ☐ 追記欄に記載した指定国

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

この欄に記載した者は、
次に該当する:

- ☐ 出願人のみである。
- ☐ 出願人及び発明者である。
- ☐ 発明者のみである。
(ここにレ印を付したときは、以下に記入しないこと)

国籍(国名):

住所(国名):

この欄に記載した者は、次の

指定国についての出願人である:

- ☐ すべての指定国 ☐ 米国を除くすべての指定国 ☐ 米国のみ ☐ 追記欄に記載した指定国

氏名(名称)及びあて名:(姓・名の順に記載;法人は公式の完全な名称を記載;あて名は郵便番号及び国名も記載)

この欄に記載した者は、
次に該当する:

- ☐ 出願人のみである。
- ☐ 出願人及び発明者である。
- ☐ 発明者のみである。
(ここにレ印を付したときは、以下に記入しないこと)

国籍(国名):

住所(国名):

この欄に記載した者は、次の

指定国についての出願人である:

- ☐ すべての指定国 ☐ 米国を除くすべての指定国 ☐ 米国のみ ☐ 追記欄に記載した指定国

☐ その他の出願人又は発明者が他の縦罫に記載されている。

第Ⅴ欄 国の指定

規則 4.9(a)の規定に基づき次の指定を行う（指定する□にレ印を付すこと：少なくとも1つの□にレ印を付すこと）。

広域申請書

- ☐ **AP** **ARIPPO** 半申請書：GH ガーナ Ghana, GM ガンビア Gambia, KE ケニア Kenya, LS レント Lesotho, MW マラウイ Malawi, SD スーダン Sudan, SL シエラ・レオネ Sierra Leone, SZ スワジランド Swaziland, TZ タンザニア United Republic of Tanzania, UG ウガンダ Uganda, ZW ジンバブエ Zimbabwe, 及びハラレプロトコルと特許協力条約の締結国である他の国
- ☐ **EA** ユーラシア半申請書：AM アルメニア Armenia, AZ アゼルバイジャン Azerbaijan, BY ベラルーシ Belarus, KG キルギス Kyrgyzstan, KZ カザフスタン Kazakhstan, MD モルドヴァ Republic of Moldova, RU ロシア Russian Federation, TJ タジキスタン Tajikistan, TM トルクメニスタン Turkmenistan, 及びユーラシア特許条約と特許協力条約の締結国である他の国
- ☒ **EP** ヨーロッパ半申請書：~~AT オーストリア Austria, BE ベルギー Belgium, CH and LI スイス及びリヒテンシュタイン Switzerland and Liechtenstein, CY キプロス Cyprus, DE ドイツ Germany, DK デンマーク Denmark, ES スペイン Spain, FI フィンランド Finland, FR フランス France, GB 英国 United Kingdom, GR ギリシャ Greece, IE アイルランド Ireland, IT イタリア Italy, LU ルクセンブルグ Luxembourg, MC モナコ Monaco, NL オランダ Netherlands, PT ポルトガル Portugal, SE スウェーデン Sweden~~, 及びヨーロッパ特許条約と特許協力条約の締結国である他の国
- ☐ **OA** **OAPI** 半申請書：BF ブルキナ・ファソ Burkina Faso, BJ ベナン Benin, CF 中央アフリカ Central African Republic, CG コンゴ Congo, CI コートジボアール Côte d'Ivoire, CM カメルーン Cameroon, GA ガボン Gabon, GN ギニア Guinea, GW ギニア・ビサウ Guinea-Bissau, ML マリ Mali, MR モーリタニア Mauritania, NE ニジェール Niger, SN セネガル Senegal, TD チャード Chad, TG トーゴ Togo, 及びアフリカ知的所有権機構のメンバー国と特許協力条約の締結国である他の国（他の種類の保護又は取扱いを求める場合には点線の上に記載する）

国内申請書（他の種類の保護又は取扱いを求める場合には点線の上に記載する）

- | | |
|--|--|
| <input type="checkbox"/> AE アラブ首長国連邦 United Arab Emirates | <input type="checkbox"/> LR リベリア Liberia |
| <input type="checkbox"/> AL アルバニア Albania | <input type="checkbox"/> LS レント Lesotho |
| <input type="checkbox"/> AM アルメニア Armenia | <input type="checkbox"/> LT リトアニア Lithuania |
| <input type="checkbox"/> AT オーストリア Austria | <input type="checkbox"/> LU ルクセンブルグ Luxembourg |
| <input type="checkbox"/> AU オーストラリア Australia | <input type="checkbox"/> LV ラトヴィア Latvia |
| <input type="checkbox"/> AZ アゼルバイジャン Azerbaijan | <input type="checkbox"/> MA モロッコ Morocco |
| <input type="checkbox"/> BA ボスニア・ヘルツェゴヴィナ Bosnia and Herzegovina | <input type="checkbox"/> MD モルドヴァ Republic of Moldova |
| | <input type="checkbox"/> MG マダガスカル Madagascar |
| <input type="checkbox"/> BB バルバドス Barbados | <input type="checkbox"/> MK マケドニア旧ユーゴスラヴィア共和国 The former Yugoslav Republic of Macedonia |
| <input type="checkbox"/> BG ブルガリア Bulgaria | |
| <input type="checkbox"/> BR ブラジル Brazil | <input type="checkbox"/> MN モンゴル Mongolia |
| <input type="checkbox"/> BY ベラルーシ Belarus | <input type="checkbox"/> MW マラウイ Malawi |
| <input type="checkbox"/> CA カナダ Canada | <input type="checkbox"/> MX メキシコ Mexico |
| <input type="checkbox"/> CH and LI スイス及びリヒテンシュタイン Switzerland and Liechtenstein | <input type="checkbox"/> NO ノルウェー Norway |
| <input checked="" type="checkbox"/> CN 中国 China | <input type="checkbox"/> NZ ニュー・ジーランド New Zealand |
| <input type="checkbox"/> CR コスタリカ Costa Rica | <input type="checkbox"/> PL ポーランド Poland |
| <input type="checkbox"/> CU キューバ Cuba | <input type="checkbox"/> PT ポルトガル Portugal |
| <input type="checkbox"/> CZ チェッコ Czech Republic | <input type="checkbox"/> RO ルーマニア Romania |
| <input type="checkbox"/> DE ドイツ Germany | <input type="checkbox"/> RU ロシア Russian Federation |
| <input type="checkbox"/> DK デンマーク Denmark | <input type="checkbox"/> SD スーダン Sudan |
| <input type="checkbox"/> DM ドミニカ Dominica | <input type="checkbox"/> SE スウェーデン Sweden |
| <input type="checkbox"/> EE エストニア Estonia | <input checked="" type="checkbox"/> SG シンガポール Singapore |
| <input type="checkbox"/> ES スペイン Spain | <input type="checkbox"/> SI スロヴェニア Slovenia |
| <input type="checkbox"/> FI フィンランド Finland | <input type="checkbox"/> SK スロヴァキア Slovakia |
| <input type="checkbox"/> GB 英国 United Kingdom | <input type="checkbox"/> SL シエラ・レオネ Sierra Leone |
| <input type="checkbox"/> GD グレナダ Grenada | <input type="checkbox"/> TJ タジキスタン Tajikistan |
| <input type="checkbox"/> GE グルジア Georgia | <input type="checkbox"/> TM トルクメニスタン Turkmenistan |
| <input type="checkbox"/> GH ガーナ Ghana | <input type="checkbox"/> TR トルコ Turkey |
| <input type="checkbox"/> GM ガンビア Gambia | <input type="checkbox"/> TT トリニダード・トバゴ Trinidad and Tobago |
| <input type="checkbox"/> HR クロアチア Croatia | <input type="checkbox"/> TZ タンザニア United Republic of Tanzania |
| <input type="checkbox"/> HU ハンガリー Hungary | <input type="checkbox"/> UA ウクライナ Ukraine |
| <input type="checkbox"/> ID インドネシア Indonesia | <input type="checkbox"/> UG ウガンダ Uganda |
| <input type="checkbox"/> IL イスラエル Israel | <input checked="" type="checkbox"/> US 米国 United States of America |
| <input type="checkbox"/> IN インド India | |
| <input type="checkbox"/> IS アイスランド Iceland | <input type="checkbox"/> UZ ウズベキスタン Uzbekistan |
| <input type="checkbox"/> JP 日本 Japan | <input type="checkbox"/> VN ヴィエトナム Viet Nam |
| <input type="checkbox"/> KE ケニア Kenya | <input type="checkbox"/> YU ユーゴスラヴィア Yugoslavia |
| <input type="checkbox"/> KG キルギス Kyrgyzstan | <input type="checkbox"/> ZA 南アフリカ共和国 South Africa |
| <input type="checkbox"/> KP 北朝鮮 Democratic People's Republic of Korea | <input type="checkbox"/> ZW ジンバブエ Zimbabwe |
| <input checked="" type="checkbox"/> KR 韓国 Republic of Korea | |
| <input type="checkbox"/> KZ カザフスタン Kazakhstan | |
| <input type="checkbox"/> LC セント・ルシア Saint Lucia | |
| <input type="checkbox"/> LK スリ・ランカ Sri Lanka | |

下の□は、この様式の施行後に特許協力条約の締結国となった国を指定するためのものである

- ☐ _____
- ☐ _____
- ☐ _____

指定の確認の宣言：出願人は、上記の指定に加えて、規則 4.9(b)の規定に基づき、特許協力条約の下で認められる他の全ての国の指定を行う。ただし、この宣言から除く旨の表示を追記欄にした国は、指定から除かれる。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15日が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。（指定の確認（料金を含む）は、優先日から15月以内に受理官庁へ提出しなければならない。）

第VI欄 優先権主張

☐ 他の優先権の主張（先の出願）が追記欄に記載されている

先の出願日 (日. 月. 年)	先の出願番号	先の出願		
		国内出願 : 国 名	広域出願 : *広域官庁名	国際出願 : 受理官庁名
(1) 12. 04. 99	平成 11 年特許願 第 1 0 3 9 9 3 号	日本国 JAPAN		
(2)				
(3)				

☐ 上記 () の番号の先の出願（ただし、本国際出願が提出される受理官庁に対して提出されたものに限る）のうち、次の () の番号のものについては、出願書類の認証書を作成し国際事務局へ送付することを、受理官庁（日本国特許庁の長官）に対して請求している。

*先の出願が、ARIPOの特許出願である場合には、その先の出願を行った工業所有権の保護のためのパリ条約同盟国の少なくとも1ヶ国を追記欄に表示しなければならない（規則4.10(b)(ii)）。追記欄を参照。

第VII欄 国際調査機関

国際調査機関（ISA）の選択

先の調査結果の利用請求：当該調査の照会（先の調査が、国際調査機関によって既に実施又は請求されている場合）

出願日（日. 月. 年）

出願番号

国名（又は広域官庁）

ISA / JP

第VIII欄 照合欄：出願の言語

この国際出願の用紙の枚数は次のとおりである。

願書 4 枚
 明細書（配列表を除く）..... 62 枚
 請求の範囲 5 枚
 要約書 1 枚
 図面 50 枚
 明細書の配列表 0 枚
 合 計 122 枚

この国際出願には、以下にチェックした書類が添付されている。

1. ☒ 手数料計算用紙
☒ 納付する手数料に相当する特許印紙を貼付した書面
☒ 国際事務局の口座への振込みを証明する書面
2. ☐ 別個の記名押印された委任状
3. ☐ 包括委任状の写し
4. ☐ 記名押印（署名）の説明書
5. ☐ 優先権書類（上記第VI欄の（ ）の番号を記載する）
6. ☐ 国際出願の翻訳文（翻訳に使用した言語名を記載する）
7. ☐ 寄託した微生物又は他の生物材料に関する書面
8. ☐ ナクレオチド又はアミノ酸配列表（フレキシブルディスク）
9. ☐ その他（書類名を詳細に記載する）

要約書とともに提示する図面： 20

本国際出願の使用言語名： 日本語

第IX欄 提出者の記名押印

各人の氏名（名称）を記載し、その次に押印する。

田 辺 恵 基

受理官庁記入欄

1. 国際出願として提出された書類の実際の受理の日

3. 国際出願として提出された書類を補完する書類又は図面であって

その後期間内に提出されたものの実際の受理の日（訂正日）

4. 特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日

5. 出願人により特定された

国際調査機関

ISA / JP

6. ☐ 調査手数料未払いにつき、国際調査機関に調査用写しを送付していない

2. 図面

☐ 受理された☐ 不足図面がある

国際事務局記入欄

記録原本の受理の日

P C T

手数料計算用紙

願書附属書

受理官庁記入欄

国際出願番号

受理官庁の日付印

出願人又は代理人の書類記号

S 00 P 0778 W O 00

出願人

ソニー株式会社 SONY CORPORATION

所定の手数料の計算

1. 及び2. 特許協力条約に基づく国際出願等に関する法律（国内法）
第18条第1項第1号の規定による手数料（注1）
（送付手数料【T】及び調査手数料【S】の合計）

95,000 円 T+S

3. 国際手数料（注2）

基本手数料

国際出願に含まれる用紙の枚数 122 枚

最初の30枚まで

46,000 円 b1

92 × 1,100 =

101,200 円 b2

30枚を超える用紙の枚数 用紙1枚の手数料

b1及びb2に記入した金額を加算し、合計額をBに記入

147,200 円 B

指定手数料

国際出願に含まれる指定数（注3） 5

5 × 9,900 =

49,500 円 D

支払うべき指定手数料
の数（上段は8）
（注4）

1指定当たりの手数料

B及びDに記入した金額を加算し、合計額をIに記入

196,700 円 I

4. 納付すべき手数料の合計

T+S及びIに記入した金額を加算し、合計額を合計に記入

291,700 円

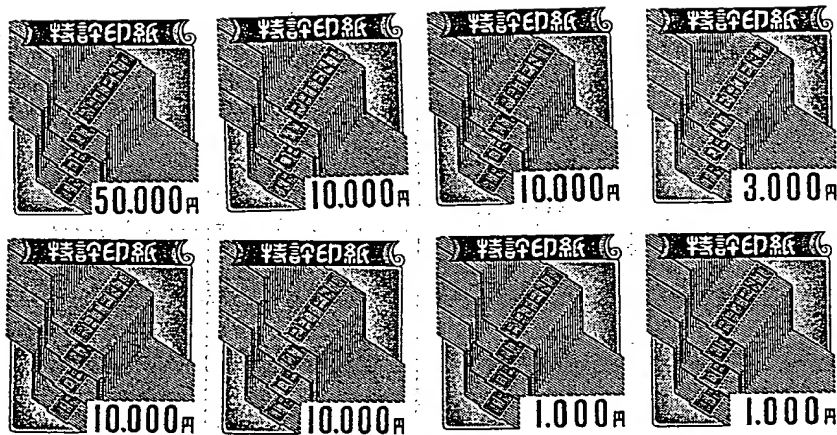
合 計

（注1）送付手数料及び調査手数料については、合計金額を特許印紙をもって納付しなければならない。

（注2）国際手数料については、受理官庁である日本国特許庁の長官が告示する国際事務局の口座への振込みを証明する書面を提出することにより納付しなければならない。

（注3）願書第V欄でレ印を付した口の数。

（注4）指定数を記入する。ただし、8指定以上は一律8とする。



送付手数料 (18,000円)
調査手数料 (77,000円)

振込日 年 月 日 00 04 07

振込金(兼消費税等込手数料)受取書

先方銀行 漢字 東京三菱

カタカナで姓と名の間はひとマスあけてください
ワイホ ビー アイー テー

濁点(・)と半濁点(゜)も一字でご記入ください
イー

おなまえ WIPO-PCT 様

おところ おでんわ(03) 3506-3856

カタカナで姓と名の間はひとマスあけてください
タナシキ モト

濁点(・)と半濁点(゜)も一字でご記入ください

市外局番 市内局番 番 号
03-3470-6570

おなまえ 田辺 東基 様

おところ 渋谷区神宮前1-11-11-508
グリーンファンタジアビル 5階

〇印をおつけください。 漢字で左づめてご記入ください

銀行 信用 信託 農協 労働 金融 他 内幸町

振込方法 〇印をおつけください。 〇電 〇文 〇信 〇書

右づめてご記入ください 0473286

金額 196,700 十億 億 千万 百万 拾万 万 千 百 拾 円

手数料 735

受取人等はカナ文字で送信しますので、フリガナは正しくていねいにご記入ください。
振込依頼書にご記入相違等の不備がありますと照会等のため振込が遅延することがあります。
午後2時以降のご用命の場合は、当日中に入金できないこともございますので、あらかじめご了承ください。
万一、通信機器・回線等の障害が生じた場合、振込が遅延したことによる補償はできませんのでご了承ください。

当行をご利用くださいますとありがとうございます。
今後ともよろしくお願い申し上げます。

当行本支店への振込のために受入れた下記の小切手等が不渡りとなったときは、その金額の振込を取消し、その小切手等は権利保全の手続きをしないで当店において返却します。

未決済小切手等

翌日発信扱

株式会社 国民銀行
原宿支店

収入印紙
振込金+手数料
3万円以上貼付
17号文書
(払戻請求書による受付
書としたものは非課税)

(為104)

基本手数料 { 147,200円 }
指定手数料 { 49,500円 }
計 196,700 円



特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 G06F 17/60	A1	(11) 国際公開番号 WO00/62216 (43) 国際公開日 2000年10月19日(19.10.00)
(21) 国際出願番号 PCT/JP00/02289 (22) 国際出願日 2000年4月7日(07.04.00) (30) 優先権データ 特願平11/103993 1999年4月12日(12.04.99) JP (71) 出願人 (米国を除くすべての指定国について) ソニー株式会社(SONY CORPORATION)[JP/J] 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo, (JP) (72) 発明者; および (75) 発明者/出願人 (米国についてのみ) 石橋義人(ISHIBASHI, Yoshihito)[JP/J] 大石丈於(OHISHI, Tateo)[JP/J] 武藤明宏(MUTO, Akihiro)[JP/J] 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo, (JP) (74) 代理人 弁理士 田辺恵基(TANABE, Shigemoto) 〒150-0001 東京都渋谷区神宮前1丁目11番11-508号 グリーンファンタジアビル5階 Tokyo, (JP)	(81) 指定国 CN, KR, SG, US, 欧州特許 (DE, FR, GB) 添付公開書類 国際調査報告書	
(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, AND PROVIDING MEDIUM (54) 発明の名称 情報処理装置および方法、並びに提供媒体 (57) Abstract It is possible to provide service according to user information. PTA-1 can be selected exclusively by a male user because "user condition 10" of "price condition 10" of PTA-1 indicates that the user is a male. PTA-2 can be selected exclusively by a female user because "user condition 20" of "price condition 20" of PTA-2 indicates that the user is a female. The amount of money indicated in the price contents of PTA-2 is half the amount of money of the corresponding PTA-1. In short, a female user can use the contents at a half price, as compared with a male user.		

11	コンテンツのID	コンテンツAのID	22
12	コンテンツのID	コンテンツAのID	23
13	UCPのID	UCPのID	24
14	サービス提供者のID	サービス提供者のID	25
15	PTのID	PTA-1のID	26
16	PTの有効期限	PTA-1の有効期限	27
17	価格条件 10	ユーザ条件 10 男性	
18	価格内容 11	2000円	30
19	価格内容 12	600円	31
20	価格内容 13	100円	32
21	価格内容 14	300円	33

PIA-1

11...ID OF CONTENTS	30...¥2,000
12...ID OF CONTENTS PROVIDER	31...¥600
13...ID OF UCP	32...¥100
14...ID OF SERVICE PROVIDER	33...¥300
15...ID OF PT	B
16...EXPIRATION OF PT	34...PRICE CONDITION 20
17...PRICE CONDITION 10	35...PRICE CONTENTS 21
18...PRICE CONTENTS 11	36...PRICE CONTENTS 22
19...PRICE CONTENTS 12	37...PRICE CONTENTS 23
20...PRICE CONTENTS 13	38...PRICE CONTENTS 24
21...PRICE CONTENTS 14	39...ID OF PTA-2
22...ID OF CONTENTS A	40...EXPIRATION OF PTA-2
23...ID OF CONTENTS PROVIDER 2-1	41...USER CONDITION 20 FEMALE
24...ID OF UCPA	42...DEVICE CONDITION 20 NONE
25...ID OF SERVICE PROVIDER 3-1	43...¥1,000
26...ID OF PTA-1	44...¥300
27...EXPIRATION OF PTA-1	45...¥50
28...USER CONDITION 10 MALE	46...¥150
29...DEVICE CONDITION 10 NONE	

11	コンテンツのID	コンテンツAのID	22
12	コンテンツのID	コンテンツAのID	23
13	UCPのID	UCPのID	24
14	サービス提供者のID	サービス提供者のID	25
15	PTのID	PTA-2のID	39
16	PTの有効期限	PTA-2の有効期限	40
17	価格条件 20	ユーザ条件 20 女性	
18	価格内容 21	1000円	43
19	価格内容 22	300円	44
20	価格内容 23	50円	45
21	価格内容 24	150円	46

PIA-2

ユーザ情報に応じてサービスを提供できるようにする。

P T A-1の「価格条件10」の「ユーザ条件10」には、男性のユーザである
とが示されているので、P T A-1は、男性のユーザのみが選択可能となる。
P T A-2の「価格条件20」の「ユーザ条件20」には、女性のユーザである
ことが示されているので、P T A-2は、女性のユーザのみが選択可能となる。
P T A-1とP T A-2の価格内容を比較すると、P T A-2の価格内容に示さ
れる額は、対応するP T A-1の価格内容に示される額の半分にされている。す
なわち、女性ユーザは、男性ユーザに比べ、半額の料金でコンテンツを利用する
ことができる。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	DM ドミニカ	KZ カザフスタン	RU ロシア
AG アンティグア・バーブーダ	DZ アルジェリア	LC セントルシア	SD スーダン
AL アルバニア	EE エストニア	LI リヒテンシュタイン	SE スウェーデン
AM アルメニア	ES スペイン	LK スリ・ランカ	SG シンガポール
AT オーストリア	FI フィンランド	LR リベリア	SI スロヴェニア
AU オーストラリア	FR フランス	LS レソト	SK スロヴァキア
AZ アゼルバイジャン	GA ガボン	LT リトアニア	SL シエラ・レオネ
BA ボスニア・ヘルツェゴビナ	GB 英国	LU ルクセンブルグ	SN セネガル
BB バルバドス	GD グレナダ	LV ラトヴィア	SZ スワジランド
BE ベルギー	GE グルジア	MA モロッコ	TD チャード
BF ブルキナ・ファソ	GH ガーナ	MC モナコ	TG トーゴ
BG ブルガリア	GM ガンビア	MD モルドヴァ	TJ タジキスタン
BJ ベナン	GN ギニア	MG マダガスカル	TM トルクメニスタン
BR ブラジル	GR ギリシャ	MK マケドニア旧ユーゴスラヴィア	TR トルコ
BY ベラルーシ	GW ギニア・ビサオ	共和国	TT トリニダード・トバゴ
CA カナダ	HR クロアチア	マリ	TZ タンザニア
CF 中央アフリカ	HU ハンガリー	MN モンゴル	UA ウクライナ
CG コンゴ	ID インドネシア	MR モーリタニア	UG ウガンダ
CH スイス	IE アイルランド	MW マラウイ	US 米国
CI コートジボアール	IL イスラエル	MX メキシコ	UZ ウズベキスタン
CM カメルーン	IN インド	MZ モザンビーク	VN ヴェトナム
CN 中国	IS アイスランド	NE ニジェール	YU ユーゴスラヴィア
CR コスタ・リカ	IT イタリア	NO ノルウェー	ZA 南アフリカ共和国
CU キューバ	JP 日本	NL オランダ	ZW ジンバブエ
CY キプロス	KE ケニア	NO ノルウェー	
CZ チェッコ	KG キルギスタン	NZ ニュージーランド	
DE ドイツ	KP 北朝鮮	PL ポーランド	
DK デンマーク	KR 韓国	PT ポルトガル	
		RO ルーマニア	

明 細 書

情報処理装置および方法、並びに提供媒体

技術分野

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

背景技術

音楽などの情報（コンテンツ）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、その情報処理装置でコンテンツを復号して、利用するシステムがある。

しかしながら、従来のシステムにおいては、ユーザの性別や年齢などの個人情報、コンテンツの利用実績、またはユーザの所有する情報処理装置の種類に応じて、コンテンツの利用を提供するなど、変化に富んだサービスを提供することができない課題があった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、変化に富んだサービスを提供することができるようにするものである。

かかる課題を解決するため本発明においては、情報処理装置において、暗号化されている第1の情報を保持する保持手段と、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を、第1の情報に対応させて記憶する記憶手段と、保持手段により保持されている暗号化されている第1の情報と、記憶手段により記憶されている第2の情報を所定の機器に送信する送信手段を具備する。

また本発明においては、情報処理方法において、暗号化されている第1の情報

を保持する保持ステップと、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を、第1の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第1の情報と、記憶ステップで記憶された第2の情報を所定の機器に送信する送信ステップを具備する。

さらに本発明においては、提供媒体において、暗号化されている第1の情報を保持する保持ステップと、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を、第1の情報に対応させて記憶する記憶ステップと、保持ステップで保持された暗号化されている第1の情報と、記憶ステップで記憶された第2の情報を所定の機器に送信する送信ステップを具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、提供媒体において、暗号化されている第1の情報が保持され、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報が、第1の情報に対応されて記憶され、保持された暗号化されている第1の情報と、記憶された第2の情報が所定のプロバイダに送信される。

さらに本発明においては、情報処理装置において、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を受信する受信手段と、受信手段により受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を作成する作成手段と、受信手段により受信された暗号化されている第1の情報および第2の情報、並びに作成手段により作成された第3の情報を、所定の機器に送信する送信手段を具備する。

さらに本発明においては、情報処理方法において、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、受信ステップで受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、受信ステップで受

信された暗号化されている第1の情報および第2の情報、並びに作成ステップで作成された第3の情報を、所定の機器に送信する送信ステップを具備する。

さらに本発明においては、提供媒体において、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、受信ステップで受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、受信ステップで受信された暗号化されている第1の情報および第2の情報、並びに作成ステップで作成された第3の情報を、所定の機器に送信する送信ステップを具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、所定のプロバイダから送信されてくる、暗号化されている第1の情報、および第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報が受信され、受信された第2の情報に対応して、第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報が作成され、受信された暗号化されている第1の情報および第2の情報、並びに作成された第3の情報が、所定の機器に送信される。

さらに本発明においては、情報処理装置において、所定の基準情報を記憶する記憶手段と、所定のプロバイダから送信されてくる、暗号化されている第1の情報、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報、および第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を受信する受信手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第2の情報の利用条件を選択する利用条件選択手段と、記憶手段に記憶されている基準情報に対応する、受信手段により受信された第3の情報の価格条件を選択する価格条件選択手段と、利用条件選択手段により選択された利用条件に対応する利用内容に従って、暗号化されている第1の情報を復号して、利用する利用手段と、価格条件選択手段により選択された価格条件に対応する価

格内容に従って、利用手段による利用に対する課金処理を実行する実行手段を具備する。

さらに本発明においては、情報処理方法において、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第1の情報、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報、および第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第2の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第3の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された利用条件に対応する利用内容に従って、暗号化されている第1の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップとを具備する。

さらに本発明においては、提供媒体において、所定の基準情報を記憶する記憶ステップと、所定のプロバイダから送信されてくる、暗号化されている第1の情報、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報、および第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報を受信する受信ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第2の情報の利用条件を選択する利用条件選択ステップと、記憶ステップで記憶された基準情報に対応する、受信ステップで受信された第3の情報の価格条件を選択する価格条件選択ステップと、利用条件選択ステップで選択された利用条件に対応する利用内容に従って、暗号化されている第1の情報を復号して、利用する利用ステップと、価格条件選択ステップで選択された価格条件に対応する価格内容に従って、利用ステップでの利用に対する課金処理を実行する実行ステップを具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、および提供媒体において、所定の基準情報が記憶され、所定のプロバイダから送信されてくる、暗号化されている第1の情報、第1の情報の利用条件と利用条件に対応する利用内容を含む第2の情報、および第1の情報の価格条件と価格条件に対応する価格内容を含む第3の情報が受信され、記憶されている基準情報に対応する、受信された第2の情報の利用条件が選択され、記憶されている基準情報に対応する、受信された第3の情報の価格条件が選択され、選択された利用条件に対応する利用内容に従って、暗号化されている第1の情報が復号され、利用され、選択された価格条件に対応する価格内容に従って、利用に対する課金処理が実行される。

図面の簡単な説明

図1は、EMDシステムを説明する系統図である。

図2は、EMDシステムにおける、主な情報の流れを説明する系統図である。

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。

図4は、EMDサービスセンタ1の配送用鍵K dの送信を説明する略線図である。

図5は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の略線図である。

図6は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の略線図である。

図7は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の略線図である。

図8は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の図表である。

図9は、システム登録情報を説明する図表である。

図10は、利用ポイント情報を説明する図表である。

図11は、コンテンツプロバイダ2の機能的構成例を示すブロック図である。

図 1 2 は、U C P の例を示す図表である。

図 1 3 は、コンテンツの管理移動を説明する略線図である。

図 1 4 は、第 1 世代複製を説明する略線図である。

図 1 5 は、サービスコードおよびコンディションコードのコード値の例を示す図表である。

図 1 6 は、U C P の利用条件として設定されたコード値の例を示す図表である。

図 1 7 は、コンテンツプロバイダセキュアコンテナの例を示す略線図である。

図 1 8 は、コンテンツプロバイダ 2 の証明書の例を示す略線図である。

図 1 9 は、サービスプロバイダ 3 の機能的構成を示すブロック図である。

図 2 0 は、P T の例を示す図表である。

図 2 1 は、P T の価格条件として設定されたコード値の例を示す図表である。

図 2 2 は、他の P T の例を示す図表である。

図 2 3 は、他の P T の価格条件として設定されたコード値の例を示す図表である。

図 2 4 は、サービスプロバイダセキュアコンテナの例を示す略線図である。

図 2 5 は、サービスプロバイダ 3 の証明書の例を示す略線図である。

図 2 6 は、ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック系統図である。

図 2 7 は、レシーバ 5 1 の S A M 6 2 の証明書の例を示す略線図である。

図 2 8 は、U C S の例を示す図表である。

図 2 9 は、レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する略線図である。

図 3 0 は、課金情報の例を示す図表である。

図 3 1 は、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図表である。

図 3 2 は、基準情報 5 1 を説明する図表である。

図 3 3 は、基準情報 5 1 の利用ポイント情報の例を示す図表である。

図 3 4 は、登録リストの例を示す図表である。

図 3 5 は、ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

図 3 6 は、レシーバ 2 0 1 の記憶モジュール 2 2 3 に記憶されている情報の例を示す図表である。

図 3 7 は、基準情報 2 0 1 の例を示す図表である。

図 3 8 は、基準情報 5 1 の利用ポイント情報の例を示す図表である。

図 3 9 は、コンテンツの利用処理を説明するフローチャートである。

図 4 0 は、EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

図 4 1 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

図 4 2 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

図 4 3 は、コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

図 4 4 は、コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図 4 5 は、サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図 4 6 は、レシーバ 5 1 がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

図 4 7 は、レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。

図 4 8 は、決済処理を説明するフローチャートである。

発明の実施の形態

以下に本発明の実施の形態を説明する。

(1) 情報配信システム

図1は、本発明を適用したEMD (E l e c t r o n i c M u s i c D i s t r i b u t i o n : 電子音楽配信) システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2、コンテンツに対応する所定のサービスを提供するサービスプロバイダ3、およびコンテンツが利用される機器（この例の場合、レシーバ51およびレシーバ201）からなるユーザホームネットワーク5から構成されている。

EMDシステムに登録された機器（例えば、レシーバ51またはレシーバ201）に配信（提供）されるコンテンツ（C o n t e n t）とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。ユーザは、コンテンツを購入し（実際は、コンテンツを利用する権利を購入し）、提供されるコンテンツを再生したり、複製して利用する。尚、コンテンツは、音楽データだけでなく、映像データ、ゲームプログラム、コンピュータプログラム、著作権データなどの場合も有りうる。

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5、および複数のコンテンツプロバイダ2（この例の場合、2つのコンテンツプロバイダ2-1, 2-2（以下、コンテンツプロバイダ2-1, 2-2を個々に区別する必要がない場合、単に、コンテンツプロバイダ2と記述する。他の装置についても同様である））に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算したり、コンテンツプロバイダ2からはUCPを、そしてサービスプロバイダ3からPTを受信する。

コンテンツプロバイダ2-1, 2-2は、提供するコンテンツ（コンテンツ鍵

K c oで暗号化されている)、そのコンテンツを復号するために必要なコンテンツ鍵K c o (配送用鍵K dで暗号化されている)、およびコンテンツの利用内容などを示す取扱方針 (以下、U C P (U s a g e C o n t r o l P o l i c y) と記述する) を保持し、それらを、コンテンツプロバイダセキュアコンテナ (後述) と称する形態で、サービスプロバイダ3に供給する。なお、この例の場合、2つのサービスプロバイダ3-1, 3-2が存在するものとする。

サービスプロバイダ3-1, 3-2は、コンテンツプロバイダ2から供給されるU C Pに対応して、1つまたは複数の価格情報 (以下、P T (P r i c e T a g) と記述する) を作成し、それを保持する。サービスプロバイダ3は、作成したP Tを、コンテンツプロバイダ2から供給されたコンテンツ (コンテンツ鍵K c oで暗号化されている)、コンテンツ鍵K c o (配送用鍵K dで暗号化されている)、およびU C Pとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

ユーザホームネットワーク5は、供給されたU C PおよびP Tに基づいて、使用許諾条件情報 (以下、U C S (U s a g e C o n t r o l S t a t u s) と称する) を作成し、作成したU C Sに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、U C Sを作成するタイミングで課金情報を作成し、例えば、配送用鍵K dの供給を受けるタイミングで、対応するU C PおよびP TなどとともにEMDサービスセンタ1に送信する。なお、ユーザホームネットワーク5は、U C PおよびP TをEMDサービスセンタ1に送信しないようにすることもできる。

この例の場合、ユーザホームネットワーク5は、図1に示すように、HDD52に接続され、SAM (S e c u r e A p p l i c a t i o n M o d u l e) 62を有するレシーバ51、およびHDD202に接続され、SAM212を有するレシーバ201から構成されている。なお、レシーバ51およびレシーバ

201 についての詳細は後述する。

(2) EMDサービスセンタ

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信したり、利益分配の情報を供給する。

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) に送信する。

鍵サーバ14は、配送用鍵Kdを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

ユーザホームネットワーク5の、EMDシステムに正式登録された機器およびコンテンツプロバイダ2に供給される、EMDサービスセンタ1からの配送用鍵Kdについて、図4乃至図7を参照して説明する。

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成する、例えば、レシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

図4の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ” の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布

されるコンテンツを暗号化するコンテンツ鍵 K_c は、バージョン1である配送用鍵 K_d で暗号化されている）であり、所定のビット数の乱数である” $b b b b b b b b$ ”の値を有するバージョン2である配送用鍵 K_d は、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵 K_c は、バージョン2である配送用鍵 K_d で暗号化されている）である。同様に、バージョン3である配送用鍵 K_d は、1998年3月中に使用可能であり、バージョン4である配送用鍵 K_d は、1998年4月中に使用可能であり、バージョン5である配送用鍵 K_d は、1998年5月中に使用可能であり、バージョン6である配送用鍵 K_d は、1998年6月中に使用可能である。

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵 K_d を送信し、コンテンツプロバイダ2は、6つの配送用鍵 K_d を受信し、記憶する。6ヶ月分の配送用鍵 K_d を記憶するのは、コンテンツプロバイダ2が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵 K_d を送信し、レシーバ51は、3つの配送用鍵 K_d を受信し、記憶する。3ヶ月の配送用鍵 K_d を記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年2月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵K dを利用できるようにするためである。

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年3月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レ

シーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdおよびバージョン2である配送用鍵Kdをそのまま記憶する。

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年4月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kd、バージョン2である配送用鍵Kd、およびバージョン3である配送用鍵Kdをそのまま記憶する。

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

このように、あらかじめ先の月の配送用鍵Kdを配布しておくことで、仮にユーザが1, 2ヶ月まったくEMDサービスセンタ1にアクセスしなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ1にアクセスして鍵を受信することができる。

また、ユーザホームネットワーク5の、EMDシステムに正式登録された機器

、およびコンテンツプロバイダ 2 には、以上のように、3 ヶ月分の配送用鍵 K d が配布されるが、EMD システムに正式登録されておらず、仮登録（詳細は後述する）されている状態の、ユーザホームネットワーク 5 の機器には、3 ヶ月分の配送用鍵 K d に代わり、図 8 に示すような、1 ヶ月分の配送用鍵 K d が配布される。この例においては、ユーザホームネットワーク 5 の機器を EMD システムに正式登録するために、与信処理など、約 1 ヶ月程度の時間を有する登録手続が必要となる。そこで、登録申請から正式登録されるまでの間（約 1 ヶ月間）においても、コンテンツの利用が可能となるように、正式登録されていない機器（仮登録されている機器）には、1 ヶ月間において利用可能な配送用鍵 K d が配布される。

図 3 に戻り、経歴データ管理部 1 5 は、ユーザ管理部 1 8 から出力される、課金情報、そのコンテンツに対応する P T、およびそのコンテンツに対応する U C P などを記憶する。

利益分配部 1 6 は、経歴データ管理部 1 5 から供給された各種情報に基づき、EMD サービスセンタ 1、コンテンツプロバイダ 2-1、2-2、およびサービスプロバイダ 3-1、3-2 の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部 1 1、コンテンツプロバイダ管理部 1 2、出納部 2 0、および著作権管理部 1 3 に出力する。利益配分部 1 6 はまた、算出した利益に応じてコンテンツプロバイダ 2-1、2-2 およびサービスプロバイダ 3-1、3-2 のそれぞれに対する利用ポイント（利益が大きければ大きいほど、すなわち、ユーザが利用すればするほど、大きい値となるポイント）を算出し、ユーザ管理部 1 8 に出力する。なお、以下において、コンテンツプロバイダ 2 における利用ポイントをコンテンツ利用ポイントと称し、サービスプロバイダ 3 における利用ポイントをサービス利用ポイントと称する。

相互認証部 1 7 は、コンテンツプロバイダ 2、サービスプロバイダ 3、およびユーザホームネットワーク 5 の機器と相互認証を実行する。

ユーザ管理部 1 8 は、EMD システムに登録可能な、ユーザホームネットワー

ク5の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図9に示すように、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に設定される情報が含まれる。

「SAMのID」には、製造された、ユーザホームネットワーク5の機器のSAMのIDが記憶される。図9のシステム登録情報の「SAMのID」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDが設定されている。

「機器番号」には、SAMを有するユーザホームネットワーク5の機器に、予め設定された機器番号が設定される。ユーザホームネットワーク5の機器が、ネットワーク4を介してサービスプロバイダ3と、およびEMDサービスセンタ1と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、UCPやPTの内容をユーザに出力（提示）したり、ユーザがUCPの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、このような機能を有する機器を主機器と称する）には、100番以上の機器番号が与えられる。機器が、そのような機能を有しない場合、その機器（以下、このような機器に従属機器と称する）には、99番以下の機器番号が与えられる。この例の場合、レシーバ51およびレシーバ201の両者は、上述した機能を有しているので、それぞれには、100番以上の機器番号（100番）が与えられてる。そこで、図9のシステム登録情報の「機器番号」には、レシーバ51のSAM62のIDおよびレシーバ201のSAM212のIDに対応する「機器番号」のそれぞれには、機器番号100番が設定されている。

「決済ID」には、EMDシステムに正式登録されたとき割り当てられる所定のIDが記憶される。この例の場合、レシーバ51は、ユーザFが決済ユーザ（後述）として、そしてレシーバ201は、ユーザAを決済ユーザとして、それぞれ正式登録され、決済IDが与えられているので、図9のシステム登録情報の、SAM62のIDおよびSAM212のIDに対応する「決済ID」には、与え

られた決済IDが設定されている。

「決済ユーザ情報」には、計上される課金を決済するユーザ（以下、このようなユーザを決済ユーザと称する）の、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ID、パスワードなどが設定される。

「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、および性別（以下、「決済ユーザ情報」に設定されるこれらの情報を、個々に区別する必要がない場合、まとめて、ユーザ一般情報と称する）は、登録が申請される際にユーザから提供され、設定されるが、この例の場合、そのうちの、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対してユーザ一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに仮登録されるときに割り当てられ、設定される。

この例の場合、レシーバ51は、ユーザFが決済ユーザとして登録されているので、図9のシステム登録情報の、SAM62のIDに対応する「決済ユーザ情報」には、ユーザFから提供されたユーザ一般情報、ユーザFのID、およびユーザFのパスワードが設定されている。レシーバ201は、ユーザAが決済ユーザとして登録されているので、SAM212のIDに対応する「決済ユーザ情報」には、ユーザAから提供されたユーザ一般情報、ユーザAのID、およびユーザAのパスワードが設定されている。なお、この例の場合、ユーザFは、男性で、ユーザAは、女性とする。

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情

報のうち、決済機関の情報以外の情報が設定される。従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよびパスワードは、仮登録または正式登録されるときに割り当てられ、設定される。

この例の場合、レシーバ51およびレシーバ201の両者には、従属ユーザが登録されていないので、図9のシステム登録情報のSAM62のIDに対応する「従属ユーザ情報」、およびSAM212のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

「利用ポイント情報」には、利益分配部16から出力された利用ポイントが設定される。図10Aは、SAM62に対応する「利用ポイント情報」に記憶されているレシーバ51の利用ポイント情報を示している。これによれば、レシーバ51のユーザF（決済ユーザ）には、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイント、コンテンツプロバイダ2-2のコンテンツ利用ポイントが123ポイント、サービスプロバイダ3-1のサービス利用ポイントが345ポイント、そしてサービスプロバイダ3-2のサービス利用ポイントが0ポイントだけ与えられている。

図10Bは、SAM212に対応する「利用ポイント情報」に記憶されているレシーバ201の利用ポイント情報を示している。これによれば、レシーバ201のユーザA（決済ユーザ）には、コンテンツプロバイダ2-1のコンテンツ利用ポイントが23ポイント、コンテンツプロバイダ2-2のコンテンツ利用ポイントが22ポイント、サービスプロバイダ3-1のサービス利用ポイントが40ポイント、そしてサービスプロバイダ3-2のサービス利用ポイントが5ポイントだけ与えられている。

なお、この例において、コンテンツプロバイダ2-1およびコンテンツプロバ

イダ 2-2 のそれぞれのコンテンツ利用ポイントの合計ポイント（ユーザ F の場合は 3 4 5（= 1 2 3 + 2 2 2））、ユーザ A の場合は 4 5 ポイント（= 2 3 + 2 2））と、サービスプロバイダ 3-1 およびサービスプロバイダ 3-2 のそれぞれのサービス利用ポイントの合計ポイント（ユーザ F の場合は 3 4 5（= 3 4 5 + 0）、ユーザ A の場合は 4 5 ポイント（= 5 + 4 0））が等しくなるようになされている。

ユーザ管理部 1 8 は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵 K d とともにユーザホームネットワーク 5 に送信する。

図 3 に、再度戻り、課金請求部 1 9 は、経歴データ管理部 1 5 から供給された、課金情報、UCP、および PT に基づき、ユーザへの課金を算出し、その結果を、出納部 2 0 に供給する。出納部 2 0 は、ユーザ、コンテンツプロバイダ 2、およびサービスプロバイダ 3 への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部 2 0 はまた、決算処理の結果をユーザ管理部 1 8 に通知する。

監査部 2 1 は、ユーザホームネットワーク 5 の機器から供給された課金情報、PT、および UCP の正当性（すなわち、不正をしていないか）を監査する。なお、この場合、EMD サービスセンタ 1 は、コンテンツプロバイダ 2 からの UCP を、サービスプロバイダ 3 からの PT を、そしてユーザホームネットワーク 5 からの UCP と PT を、それぞれ受け取る。

（3）コンテンツプロバイダ

図 1 1 は、コンテンツプロバイダ 2-1 の機能的構成を示すブロック図である。コンテンツサーバ 3 1 は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部 3 2 に供給する。ウォーターマーク付加部 3 2 は、コンテンツサーバ 3 1 から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部 3 3 に供給する。

圧縮部 3 3 は、ウォーターマーク付加部 3 2 から供給されたコンテンツを、AT

RAC2 (Adaptive Transform Acoustic Coding 2) (商標) 等の方式で圧縮し、暗号化部34に供給する。暗号化部34は、圧縮部33で圧縮されたコンテンツを、乱数発生部35から供給された乱数を鍵（以下、この乱数をコンテンツ鍵 K_{co} と称する）として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

乱数発生部35は、コンテンツ鍵 K_{co} となる所定のビット数の乱数を暗号化部34および暗号化部36に供給する。暗号化部36は、コンテンツ鍵 K_{co} をEMDサービスセンタ1から供給された配送用鍵 K_d を使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の64ビットは、上位32ビットの H_0 、および下位32ビットの L_0 に分割される。鍵処理部から供給された48ビットの拡大鍵 K_1 、および下位32ビットの L_0 を入力とし、下位32ビットの L_0 を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの H_0 と、F関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

上位32ビットの H_0 および下位32ビットの L_0 を基に、以上の処理を16回繰り返し、得られた上位32ビットの H_{16} および下位32ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

ポリシー記憶部 37 は、コンテンツに対応して設定される UCP を記憶し、セキュアコンテナ作成部 38 に出力する。図 12 は、コンテンツサーバ 31 に保持されているコンテンツ A に対応して設定され、ポリシー記憶部 37 に記憶されている UCP A、B を表している。UCP には、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「利用条件」、「利用内容」の各項目に設定される情報が含まれる。「コンテンツの ID」には、UCP が対応するコンテンツの ID が設定される。UCP A (図 12 A) および UCP B (図 12 B) のそれぞれの「コンテンツの ID」には、コンテンツ A の ID が設定されている。

「コンテンツプロバイダの ID」には、コンテンツの提供元のコンテンツプロバイダの ID が設定される。UCP A および UCP B のそれぞれの「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2-1 の ID が設定されている。「UCP の ID」には、各 UCP に割り当てられた所定の ID が設定され、UCP A の「UCP の ID」には、UCP A の ID が、UCP B の「UCP の ID」には、UCP B の ID が、それぞれ設定されている。「UCP の有効期限」には、UCP の有効期限を示す情報が設定され、UCP A の「UCP の有効期限」には、UCP A の有効期限が、UCP B の「UCP の有効期限」には、UCP B の有効期限が、それぞれ設定されている。

「利用条件」は、「ユーザ条件」および「機器条件」の項目からなり、「ユーザ条件」には、この UCP を選択することができるユーザの条件が設定され、「機器条件」には、この UCP を選択することができる機器の条件が設定される。

UCP A の場合、「利用条件 10」が設定され、「利用条件 10」の「ユーザ条件 10」には、利用ポイントが 200 ポイント以上であることが条件であることを示す情報（“200 ポイント以上”）が設定されている。また「利用条件 10」の「機器条件 10」には、条件がないことを示す情報（“条件なし”）が設定されている。すなわち、UCP A は、200 ポイント以上のコンテンツプロバイダ 2-1 のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

UCPBの場合、「利用条件20」が設定され、「利用条件20」の「ユーザ条件20」には、利用ポイントが200ポイントより少ないことが条件であることを示す情報（”200ポイントより少ない”）が設定されている。また「利用条件20」の「機器条件20」には、”条件なし”が設定されている。すなわち、UCPBは、200ポイントより少ないコンテンツプロバイダ2-1のコンテンツ利用ポイントを有するユーザのみが選択可能となる。

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」などの項目からなり、その「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報（”可”または”不可”）が設定されている。コンテンツの管理移動が行われると、図13Aに示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図13Bに示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図13Aに示すように、他の機器にコンテンツを管理移動することができない（許可されていない）。すなわち、管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。この点で、図14Aに示すように、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図14Bに示すように、1回だけの複製とも異なる。

図12Aに戻り、UCPAには、4つの「利用内容11」乃至「利用内容14」が設けられており、「利用内容11」において、その「ID11」には、「利用内容11」に割り当てられた所定のIDが設定されている。「形式11」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ11」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報11」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

「利用内容12」において、その「ID12」には、「利用内容12」に割り当てられた所定のIDが設定されている。「形式12」には、第1世代の複製を行う利用形式を示す情報（”第1世代複製”）が設定されている。第1世代複製は、図14Aに示したように、オリジナルのコンテンツから、複数の第1世代の複製を作成することができる。ただし、第1世代の複製から第2世代の複製を作成することはできない（許可されていない）。「パラメータ12」には、”第1世代複製”に対応する所定の情報が設定されている。「管理移動許可情報12」には、コンテンツの管理移動が許可されていないことを示す”不可”が設定されている。

「利用内容13」において、その「ID13」には、「利用内容13」に割り当てられた所定のIDが設定されている。「形式13」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ13」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報13」には、”不可”が設定されている。

「利用内容14」において、その「ID14」には、「利用内容14」に割り当てられた所定のIDが設定されている。「形式14」には、5回の複製を行う利用形式（いわゆる、5回複製することができる回数券）を示す情報（”Pay Per Copy 5”）が設定されている。なお、この場合も、図14のBに示すように、複製からの複製を作成することはできない（許可されていない）。「パラメータ14」には、”Pay Per Copy 5”に対応して、複製が5回可能

であることを示す情報”複製5回”が設定されている。「管理移動許可情報14」には、”不可”が設定されている。

図12BのUCPBには、2つの「利用内容21」および「利用内容22」が設けられている。「利用内容21」において、その「ID21」には、「利用内容21」に割り当てられた所定のIDが設定されている。「形式21」には、4回の再生を行う利用形式を示す情報（”Pay Per Play4”）が設定され、「パラメータ21」には、再生が4回可能であることを示す情報（”再生4回”）が設定されている。「管理移動許可情報21」には、”不可”が設定されている。

「利用内容22」において、その「ID22」には、「利用内容22」に割り当てられた所定のIDが設定されている。「形式22」には、”Pay Per Copy2”が設定され、「パラメータ22」には、”複製2回”が設定されている。「管理移動許可情報22」には、”不可”が設定されている。

ここで、UCPAおよびUCPBの内容を比較すると、200ポイント以上の利用ポイントを有するユーザは、4通りの利用内容11乃至利用内容14から利用内容を選択することができるのに対して、200ポイントより少ない利用ポイントを有するユーザは、2通りの利用内容21、22からしか利用内容を選択することができないものとされている。

ところで、図12は、UCPAおよびUCPBを模擬的に表しているが、例えば、UCPAの「利用条件10」およびUCPBの「利用条件20」は、図15Aに示すサービスコード、および図15Bに示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードにより、実際は構成されている。

図16Aは、UCPA（図12A）の「利用条件10」の「ユーザ条件10」および「機器条件10」として設定されている各コードのコード値を表している。UCPAの「利用条件10」の「ユーザ条件10」は、”200ポイント以上”とされているので、”利用ポイントに関し条件有り”を意味する80xxhのサー

ビスコード (図 15 A) が、このとき数値 200 を示す 0000C8h のバリューコードが、そして” >= (以上)” を意味する 06h のコンディションコード (図 15 B) が、ユーザ条件として設定されている。

UCPA の「機器条件 10」は、” 条件なし” とされているので、” 条件なし” を意味する 0000h のサービスコードが、このとき何ら意味を持たない FFF FFFh のバリューコードが (図 15 A)、そして” 無条件” を意味する 00h のコンディションコード (図 15 B) が、機器条件として設定されている。

図 16 B は、UCPB の「利用条件 20」の「ユーザ条件 20」および「機器条件 20」として設定されている各コードのコード値を表している。「ユーザ条件 20」は、” 200 ポイントより少ない” とされているので、” 利用ポイントに関し条件有り” を意味する 80xxh のサービスコードが、数値 200 を示す 0000C8h のバリューコード (図 15 A) が、そして” < (より小さい)” を意味する 03h のコンディションコード (図 15 B) が、ユーザ条件として設定されている。

UCPB の「機器条件 20」は、UCPA の「機器条件 10」と同様に、” 条件なし” とされ、同一のコード値が設定されているので、その説明は省略する。

図 11 に戻り、セキュアコンテナ作成部 38 は、例えば、図 17 に示すような、コンテンツ A (コンテンツ鍵 KcoA で暗号化されている)、コンテンツ鍵 KcoA (配送用鍵 Kd で暗号化されている)、UCPA, B、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ (この場合、コンテンツ A (コンテンツ鍵 KcoA で暗号化されている)、コンテンツ鍵 KcoA (配送用鍵 Kd で暗号化されている)、および UCPA, B の全体) にハッシュ関数を適用して得られたハッシュ値が、コンテンツプロバイダの公開鍵暗号の秘密鍵 (この場合、コンテンツプロバイダ 2-1 の秘密鍵 Kscp) で暗号化されたものである。

セキュアコンテナ作成部 38 はまた、コンテンツプロバイダセキュアコンテナに、図 18 に示すコンテンツプロバイダ 2-1 の証明書を付してサービスプロバ

イダ3に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2-1に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ2-1の名前、コンテンツプロバイダ2-1の公開鍵 K_{pcp} 、並びにその署名（認証局の秘密鍵 K_{sca} で暗号化されている）から構成されている。

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値を取り、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD (Message Digest) 4, MD5, SHA (Secure Hash Algorithm) -1などが用いられる。

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的な RSA (R i v e s t - S h a m i r - A d l e m a n) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める (すなわち、 e と L を共通に割り切れる数は、1のみである)。

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $e d = 1 \pmod{L}$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p 、 q 、および d が、秘密鍵とされる。

暗号文 C は、平文 M から、式 (1) の処理で算出される。

$$C = M^e \pmod{n} \quad (1)$$

暗号文 C は、式 (2) の処理で平文 M に、復号される。

$$M = C^d \pmod{n} \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式 (3) が成立するからである。

$$M = C^d = (M^e)^d = M^{e d} = M \pmod{n} \quad (3)$$

秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異

なる鍵とすることができる。

また、公開鍵暗号の他の例である楕円曲線暗号 (Elliptic Curve Cryptography) についても、簡単に説明する。楕円曲線 $y^2 = x^3 + ax + b$ 上の、ある点を B とする。楕円曲線上の点の加算を定義し、 nB は、 B を n 回加算した結果を表す。同様に、減算も定義する。 B と nB から n を算出することは、困難であることが証明されている。 B と nB を公開鍵とし、 n を秘密鍵とする。乱数 r を用いて、暗号文 $C1$ および $C2$ は、平文 M から、公開鍵で式 (4) および式 (5) の処理で算出される。

$$C1 = M + r n B \quad (4)$$

$$C2 = r B \quad (5)$$

暗号文 $C1$ および $C2$ は、式 (6) の処理で平文 M に、復号される。

$$M = C1 - n C2 \quad (6)$$

復号できるのは、秘密鍵 n を有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図11に、再び戻り、コンテンツプロバイダ2-1の相互認証部39は、EMDサービスセンタ1から配送用鍵 K_d の供給を受けるのに先立ち、EMDサービスセンタ1と相互認証し、また、相互認証部39は、サービスプロバイダ3へのコンテンツセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密にしなければならない情報が含まれていないので、この相互認証は、必ずしも必要とされない。

コンテンツプロバイダ 2-2 は、コンテンツプロバイダ 2-1 と基本的の同様の構成を有しているので、その図示および説明は省略する。

(4) サービスプロバイダ

次に、図 19 のブロック図を参照して、サービスプロバイダ 3-1 の機能的構成を説明する。コンテンツサーバ 4-1 は、コンテンツプロバイダ 2 から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ (コンテンツ鍵 K_{co} で暗号化されている)、コンテンツ鍵 K_{co} (配送用鍵 K_d で暗号化されている)、UCP、およびコンテンツプロバイダ 2 の署名を記憶し、セキュアコンテナ作成部 4-4 に供給する。

値付け部 4-2 は、コンテンツプロバイダ 2 から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ 2 の証明書が検証され、正当であるとき、コンテンツプロバイダ 2 の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部 4-2 は、コンテンツプロバイダセキュアコンテナに含まれる UCP に対応する、PT を作成し、セキュアコンテナ作成部 4-4 に供給する。図 20 は、図 12A の UCPA に対応して作成された、2 つの PTA-1 (図 20A) および PTA-2 (図 20B) を表している。PT には、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「サービスプロバイダの ID」、「PT の ID」、「PT の有効期限」、「価格条件」、および「価格内容」の各項目に設定される情報が含まれる。

PT の、「コンテンツの ID」、「コンテンツプロバイダの ID」、および「UCP の ID」には、UCP に対応する各項目の情報が、それぞれ設定される。すなわち、PTA-1 および PTA-2 のそれぞれの「コンテンツの ID」には、コンテンツ A の ID が、それぞれの「コンテンツプロバイダの ID」には、コンテ

ンツプロバイダ 2-1 の ID が、そしてそれぞれの「UCP の ID」には、UCPA の ID が設定されている。

「サービスプロバイダの ID」には、PT の提供元のサービスプロバイダ 3 の ID が設定される。PTA-1 および PTA-2 の「サービスプロバイダの ID」には、サービスプロバイダ 3-1 の ID が設定されている。「PT の ID」には、各 PT に割り当てられた所定の ID が設定される。PTA-1 の「PT の ID」には、PTA-1 の ID が、PTA-2 の「PT の ID」には、PTA-2 の ID がそれぞれ設定されている。「PT の有効期限」には、PT の有効期限を示す情報が設定される。PTA-1 の「PT の有効期限」には、PTA-1 の有効期限が、PTA-2 の「PT の有効期限」には、PTA-2 の有効期限が設定されている。

「価格条件」は、UCP の「利用条件」と同様に、「ユーザ条件」および「機器条件」の項目からなり、その「ユーザ条件」には、この PT を選択することができるユーザの条件が設定され、その「機器条件」には、この PT を選択することができる機器の条件が設定される。

PTA-1 の場合、「価格条件 10」が設定され、「価格条件 10」の「ユーザ条件 10」には、ユーザが男性であることを示す情報（“男性”）が設定され、その「機器条件 10」には、“条件なし”が設定されている。すなわち、PTA-1 は、男性のユーザのみが選択可能となる。

PTA-1 の「価格条件 10」の「ユーザ条件 10」および「機器条件 10」も、実際は、図 21A に示すように、各種コードのコード値が設定されている。

「価格条件 10」の「ユーザ条件 10」には、“性別条件有り”を意味する 01 x x h のサービスコード（図 15A）が、このとき男性を意味する 000000 h のバリューコードが、そして“=”を意味する 01 h のコンディションコード（図 15B）が設定されている。「機器条件 10」には、“条件なし”を意味する 0000 h のサービスコードが、この場合何ら意味を持たない F F F F F F h のバリューコードが、そして“無条件”を意味する 00 h のコンディションコード

が設定されている。

P T A-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ条件20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件20」には、”条件なし”が設定されている。すなわち、P T A-2は、女性のユーザのみが選択可能となる。

P T A-2の「価格条件20」の「ユーザ条件20」および「機器条件20」も、実際は、図21Bに示すように、各コードのコード値が設定されている。「価格条件20」の「ユーザ条件20」には、”性別条件有り”を意味する01xxhのサービスコード（図15A）が、この場合女性を示す000001hのバリューコードが、そして”=”を意味する01hのコンディションコード（図15B）が設定されている。その「機器条件20」には、”条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

図20に戻り、P Tの「価格内容」には、コンテンツが、対応するU C Pの「利用内容」の「形式」に設定された利用形式で利用される場合の利用料金が示されている。すなわち、P T A-1の「価格内容11」に設定された”2000円”およびP T A-2の「価格内容21」に設定された”1000円”は、U C P A（図12A）の「利用内容11」の「形式11」が”買い取り再生”とされているので、コンテンツAの買い取り価格（料金）を示している。

P T A-1の「価格内容12」の”600円”およびP T A-2の「価格内容22」の”300円”は、U C P Aの「利用内容12」の「形式12」より、第1世代複製の利用形式でコンテンツAを利用する場合の料金を示している。P T A-1の「価格内容13」の”100円”およびP T A-2の「価格内容23」の”50円”は、U C P Aの「利用内容13」の「形式13」より、期間制限再生の利用形式でコンテンツAを利用する場合の料金を示している。P T A-1の「価格内容14」の”300円”およびP T A-2の「価格内容24」の”15

0円”は、UCPAの「利用内容14」の「形式14」より、5回の複製を行う利用形式でコンテンツAを利用する場合の料金を示している。

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1の価格内容に示される価格が、PTA-2の価格内容に示される価格の2倍に設定されている。例えば、UCPAの「利用内容11」に対応するPTA-1の「価格内容11」が”2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は”1000円”とされている。同様、PTA-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格のそれぞれの2倍とされている。すなわち、女性ユーザは、男性ユーザに比べ、コンテンツAを、半額の料金で利用することができる。

図22は、図12BのUCPBに対応して作成された、2つのPTB-1およびPTB-2を表している。図22AのPTB-1には、コンテンツAのID、コンテンツプロバイダ2-1のID、UCPBのID、UCPBの有効期限、サービスプロバイダ3-1のID、PTB-1のID、PTB-1の有効期限、価格条件30、2通りの価格内容31、32などが含まれている。

PTB-1の「価格条件30」の「ユーザ条件30」には”条件なし”が設定され、「機器条件30」には、機器が従機器であることを示す情報（”従機器”）が設定されている。すなわち、PTB-1は、コンテンツAが従機器において利用される場合にのみ選択可能となる。

PTB-1の「価格条件30」の「ユーザ条件30」および「機器条件30」にも、実際は、図23Aに示すように、各コードのコード値が設定されている。

「ユーザ条件30」には、”条件なし”を意味する0000hのサービスコード（図15A）が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード（図15B）が設定されている。「機器条件30」は、”従機器”とされているので、”機器に関

し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”< (小さい)”を意味する03hのコンディションコードが設定されている。この例の場合、従機器には、100番より小さい機器番号が設定されているので、このようなコード値が設定される。

PTB-1の「価格内容31」の”100円”は、UCPB (図12B)の「利用内容21」の「形式21」が”Pay Per Play 4”とされているので、4回の再生を行う場合の料金を示し、「価格内容32」の”300円”は、UCPBの「利用内容22」の「形式22」が”Pay Per Copy 2”とされているので、2回の複製を行う場合の料金を示している。

UCPBに対応して作成された、もう一方の図22BのPTB-2には、コンテンツAのID、コンテンツプロバイダ2-1のID、UCPBのID、サービスプロバイダ3-1のID、PTB-2のID、PTB-2の有効期限、価格条件40、および2通りの価格内容41、42などが含まれている。

PTB-2の「価格条件40」の「ユーザ条件40」には”条件なし”が設定され、その「機器条件40」には、機器が主機器であることを条件とする情報(”主機器”)が設定されている。すなわち、PTB-2は、主機器においてコンテンツAが利用される場合にのみ選択可能となる。

PTB-2の「価格条件40」の「ユーザ条件40」および「機器条件40」にも、実際は、図23Bに示すように、各コードのコード値が設定されている。

「価格条件40」の「ユーザ条件40」には、”条件なし”を意味する0000hのサービスコード(図15A)が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード(15B)が設定されている。「機器条件40」には、”機器に関し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”=> (以上)”を意味する06hのコンディションコードが設定されている。

P T B - 2 の「価格内容 4 1」および「価格内容 4 2」のそれぞれに示される価格は、U C P B の「利用内容 2 1」の「形式 2 1」および「利用内容 2 2」の「形式 2 2」のそれぞれに示される利用形式でコンテンツ A を利用する場合の料金を示している。

ここで、P T B - 1（従機器に適用される）の価格内容と P T B - 2（主機器に適用される）の価格内容を比較すると、P T B - 1 の価格内容は、P T B - 2 の価格内容の 2 倍に設定されている。例えば、P T B - 1 の「価格内容 3 1」が” 1 0 0 円”とされているのに対し、P T B - 2 の「価格内容 4 1」は 5 0 円とされており、「価格内容 3 2」が” 3 0 0 円”とされているのに対して、「価格内容 4 2」は” 1 5 0 円”とされている。

図 1 9 に戻り、ポリシー記憶部 4 3 は、コンテンツプロバイダ 2 から供給された、コンテンツの U C P を記憶し、セキュアコンテナ作成部 4 4 に供給する。

セキュアコンテナ作成部 4 4 は、例えば、図 2 4 に示すような、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、U C P A、B、コンテンツプロバイダ 2 の署名、P T A - 1、A - 2、B - 1、B - 2、およびサービスプロバイダ 3 の署名からなるサービスプロバイダセキュアコンテナを作成する。

セキュアコンテナ作成部 4 4 はまた、作成したサービスプロバイダセキュアコンテナを、図 2 5 に示すような、証明書のバージョン番号、認証局がサービスプロバイダ 3 - 1 に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ 3 - 1 の名前、サービスプロバイダ 3 - 1 の公開鍵 K p s p、並びに認証局の署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク 5 に供給する。

図 1 9 に、再び戻り、相互認証部 4 5 は、コンテンツプロバイダ 2 からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ 2 と相互認証する。相互認証部 4 5 また、ユーザホームネットワーク 5 へ

のサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク 5 と相互認証するが、このサービスプロバイダ 3 とユーザホームネットワーク 5 との相互認証は、例えば、ネットワーク 4 が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ 3 は、コンテンツプロバイダ 2 およびユーザホームネットワーク 5 と相互認証を行わなくてもよい。

サービスプロバイダ 3-2 の構成は、サービスプロバイダ 3-1 の構成と基本的に同様であるので、その図示および説明は省略する。

(5) ユーザホームネットワーク

(5-1) レシーバ 5 1

次に、図 26 のブロック図を参照して、ユーザホームネットワーク 5 を構成するレシーバ 5 1 の構成例を説明する。レシーバ 5 1 は、通信部 6 1、SAM 6 2、外部記憶部 6 3、伸張部 6 4、通信部 6 5、インタフェース 6 6、表示制御部 6 7、および入力制御部 6 8 より構成されている。通信部 6 1 は、ネットワーク 4 を介してサービスプロバイダ 3、または EMD サービスセンタ 1 と通信し、所定の情報を受信し、または送信する。

SAM 6 2 は、相互認証モジュール 7 1、課金処理モジュール 7 2、記憶モジュール 7 3、復号/暗号化モジュール 7 4、およびデータ検査モジュール 7 5 からなるが、シングルチップの暗号処理専用 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

SAM 6 2 の相互認証モジュール 7 1 は、記憶モジュール 7 3 に記憶されている、図 27 に示す SAM 6 2 の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵 K_{temp} （セッション鍵）を復号/暗号化モジュール 7 4 に供給する。SAM の証明書には、コン

テンツプロバイダ 2-1 の証明書 (図 18) およびサービスプロバイダ 3-1 の証明書 (図 25) に含まれている情報に対応する情報が含まれているので、その説明は省略する。

課金処理モジュール 72 は、選択された UCP の利用内容に基づいて、使用許諾条件情報 UCS および課金情報を作成する。図 28 は、コンテンツが “買い取り再生” の利用形式で権利購入された場合の UCS の例であり、図 12A に示した UCPA の利用内容 11 と、図 20A に示した PTA-1 に基づいて作成された UCSA を表している。UCS には、図 28 に示されるように、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「サービスプロバイダの ID」、「PT の ID」、「PT の有効期限」、「UCS の ID」、「SAM の ID」、「ユーザの ID」、「利用内容」、および「利用履歴」などの項目に設定される情報が含まれている。

UCS の、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「サービスプロバイダの ID」、「PT の ID」、および「PT の有効期限」の各項目には、PT の、それらに対応する項目の情報が設定される。すなわち、図 28 の UCSA の、「コンテンツの ID」には、コンテンツ A の ID が、「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2-1 の ID が、「UCP の ID」には、UCPA の ID が、「UCP の有効期限」には、UCPA の有効期限が、「サービスプロバイダの ID」には、サービスプロバイダ 3-1 の ID が、「PT の ID」には、PTA-1 の ID が、そして「PT の有効期限」には、PTA-1 の有効期限が、それぞれ設定されている。

「UCS の ID」には、UCS に割り当てられた所定の ID が設定され、UCSA の「UCS の ID」には、UCSA の ID が設定されている。「SAM の ID」には、機器の SAM の ID が設定され、UCSA の「SAM の ID」には、レシーバ 51 の SAM 62 の ID が設定されている。「ユーザの ID」には、コンテンツを利用するユーザの ID が設定され、UCSA の「ユーザの ID」には、ユーザ F の ID が設定されている。

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」などの項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容11」の「ID11」に設定されている情報（利用内容11のID）が、「形式」には、「利用内容11」の「形式11」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容11」の「パラメータ11」に設定されている情報（”買い取り再生”に対応する情報）が設定される。

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDと管理移動先の機器のIDは、共に、管理移動元の機器のIDとされる。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には、”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われず（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容11」の「管理移動許可情報11」に”可”が設定されており、また、このとき、コンテンツAは管理移動されていないので、SAM62のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

「利用履歴」には、同一のコンテンツに対する利用履歴が含まれている。UCSAの「利用履歴」には、”買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ51において、コンテンツAが以前に利用されていた場合、そのときの利用形式を示す情報も記憶されている。

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述したUCSにおいて、「コンテンツプロバイダのID」が設けられてい

るが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

作成されたUCSは、レシーバ51の復号/暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図29に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

図29の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図28に示したUCSAと、コンテンツAを復号するためのコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1, RP-2には、他のコンテンツ鍵Kco1, Kco2（それぞれ保存用鍵Ksaveで暗号化されている）およびUCS1, 2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4（図示せず）乃至RP-N、およびブロックBP-2（図示せず）乃至BP-Mには、コンテンツ鍵KcoおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域RPに記憶されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

図30は、図28に示したUCSAと同時に作成された課金情報Aを表してい

る。課金情報には、図30に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」などの項目に設定される情報が含まれている。

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定されている。すなわち、図30の課金情報Aの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2-1のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3-1のIDが、「PTのID」には、PTA-1のIDが、「PTの有効期限」には、PTA-1の有効期限が、「UCSのID」には、UCSAのIDが、「SAMのID」には、SAM62のIDが、「ユーザのID」には、ユーザFのIDが、そして「利用内容」には、UCSAの「利用内容11」の内容が、それぞれ設定されている。

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報などが設定される。課金情報Aの「課金履歴」には、レシーバ51において計上された課金の合計額が設定されている。

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述した課金情報において、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サー

ビスプロバイダを特定することができる場合、それを設けないようにすることもできる。

図26に戻り、記憶モジュール73には、図31に示すように、SAM62の公開鍵 K_{pu} 、SAM62の秘密鍵 K_{su} 、EMDサービスセンタ1の公開鍵 K_{pesc} 、認証局の公開鍵 K_{pca} 、保存用鍵 K_{save} 、3ヶ月分の配送用鍵 K_d などの各種鍵、SAM62の証明書(図27)、課金情報(例えば、図30の課金情報Aなど)、基準情報51、およびM個の検査値 $HP-1$ 乃至 $HP-M$ などが記憶されている。

図32は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定の情報などが含まれている。

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の項目には、EMDサービスセンタ1のユーザ管理部18により管理されるシステム登録情報(図9)の、それらに対応する項目の情報が設定される。すなわち、基準情報51には、SAM62のID、SAM62の機器番号(100番)、ユーザFの決済ID、ユーザFの決済ユーザ情報(ユーザFのユーザ一般情報(氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザFのID、およびユーザFのパスワード)、および図33に示す利用ポイント情報(図10A)に示したものと同様の情報)が設定されている。

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる額が、課金の上限額として設定される。基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額(正式登録時の上限額)が設定されている。なお、正式登録されている状態における課金の上限額は、仮登録されている状態における課金の上限額よりも、大きな額である。

次に、記憶モジュール73に記憶される、図31に示したM個の検査値 $HP-1$ 乃至 $HP-M$ について説明する。検査値 $HP-1$ は、外部記憶部63の利用情報記憶部63A（図29）のブロック $BP-1$ に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値 $HP-2$ 乃至 $HP-M$ も、検査値 $HP-1$ と同様に、外部記憶部63の、対応するブロック $BP-2$ 乃至 $BP-M$ のそれぞれに記憶されているデータのハッシュ値である。

図26に戻り、SAM62の復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵 Kc_o を配送用鍵 Kd で復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、必要に応じて（例えば、相互認証時）、所定の桁数の乱数を発生して一時鍵 $Ktemp$ を生成し、暗号化ユニット93に出力する。

暗号化ユニット93は、復号されたコンテンツ鍵 Kc_o を、再度、記憶モジュール73に保持されている保存用鍵 $Ksave$ で暗号化する。暗号化されたコンテンツ鍵 Kc_o は、外部記憶部63に供給される。暗号化ユニット93は、コンテンツ鍵 Kc_o を伸張部64に送信するとき、コンテンツ鍵 Kc_o を乱数発生ユニット92で生成した一時鍵 $Ktemp$ で暗号化する。

データ検査モジュール75は、記憶モジュール73に記憶されている検査値 HP と、外部記憶部63の利用情報記憶部63Aの、対応するブロック BP のデータのハッシュ値を比較し、ブロック BP のデータが改竄されていないか否かを検査する。データ検査モジュール75はまた、コンテンツの購入、移動、および管理移動等が行われる際に、検査値 HP を再算出し、記憶モジュール73に記憶（更新）させる。

伸張部64は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォーターマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62と相互認証し、一時鍵 $Ktemp$ を復号モジュール102に出力する。復号モジュール102は

、一時鍵K t e m p で暗号化されたコンテンツ鍵K c oを一時鍵K t e m p で復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵K c oで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATRA C2等の方式で伸張し、ウォーターマーク付加モジュール105に出力する。ウォーターマーク付加モジュール105は、コンテンツにレシーバ51を特定するための情報（例えば、SAM62のID）のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

通信部65は、ユーザホームネットワーク5のレシーバ201との通信処理を行う。インターフェース66は、SAM62および伸張部64からの信号を所定の形式に変更し、HDD52に出力し、また、HDD52からの信号を所定の形式に変更し、SAM62および伸張部64に出力する。

表示制御部67は、表示部（図示せず）への出力を制御する。入力制御部68は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

HDD52は、サービスプロバイダ3から供給されたコンテンツ、UCP、およびPTの他、図34に示すような、登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ51のSAM62のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51には、他の機器が接続されていないので、自分自身を含む値1が（「接続されている機器数」の欄に）記憶されている。

リスト部は、「SAM ID」、「ユーザID」、「購入処理」、「課金処理」、「課

金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件として、それぞれの項目に所定の情報が記憶されている。

「SAM ID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のIDが記憶されている。「ユーザID」には、対応する機器のユーザのIDが記憶される。この例の場合、ユーザFのIDが記憶されている。

「購入処理」には、コンテンツを購入するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ51は、コンテンツを購入するための処理を行うことができるので、”可”が記憶されている。

「課金処理」には、EMDサービスセンタ1との間で、課金を決済する処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ51は、ユーザFが決済ユーザとして登録されているので、課金を決済する処理を行うことができる。そのため、「課金処理」には、”可”が記憶されている。

「課金機器」には、計上された課金に対する課金処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51（SAM62）は、自分自身が、課金を決済することができるので、SAM62のIDが記憶されている。

「コンテンツ供給機器」には、対応する機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51は、コンテンツの供給をサービスプロバイダ3から受けるので、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。

「状態フラグ」には、対応する機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止させられている

場合には、その旨を示す情報（”停止”）が記憶される。例えば、決済が成功しなかった場合や、正式登録されるための与信処理が完了していない場合（仮登録されている場合）、「状態フラグ」には、”制限あり”が設定される。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツを利用する処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

この例の場合、レシーバ51に対しては、何ら制限が課せられていないものとし、「状態フラグ」には”なし”が設定されている。

「登録条件署名」には、登録条件として、それぞれ、「SAM ID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。この例の場合、レシーバ51の登録条件に対する署名が記憶されている。「登録リスト署名」には、登録リストに設定されたデータの全体に対する署名が設定されている。

（5-2）レシーバ201

図35は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その説明は適宜省略する。

SAM212の記憶モジュール223にも、図36に示すように、SAM212の公開鍵 K_{pu} 、SAM212の秘密鍵 K_{su} 、EMDサービスセンタ1の公開鍵 K_{psc} 、認証局の公開鍵 K_{pca} 、保存用鍵 K_{save} 、3月分の配送用鍵 K_d 、予め認証局から配布されているSAM212の証明書、および基準情報201が記憶されている。基準情報201には、図37に示すように、SAM212のID、レシーバ201の機器番号（100番）、ユーザAの決済ID、ユ

ーザAの決済ユーザ情報（ユーザAのユーザ一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザAのID、およびユーザAのパスワード）、および図38に示す利用ポイント情報（図10Bに示したものと同様の情報）が設定されている。

HDD202は、HDD52と同様の機能を有するので、その説明は省略する。

（6）コンテンツの購入及び利用

次に、EMDシステムの処理について、図39のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ2-1に保持されているコンテンツAが、サービスプロバイダ3-1を介して、ユーザホームネットワーク5のレシーバ51に供給され、利用される場合を例として説明する。

（6-1）EMDサービスセンタからコンテンツプロバイダへの配送用鍵の伝送
ステップS11において、配送用鍵Kdが、EMDサービスセンタ1からコンテンツプロバイダ2-1に供給される処理が行われる。この処理の詳細は、図40のフローチャートに示されている。すなわち、ステップS31において、EMDサービスセンタ1の相互認証部17は、コンテンツプロバイダ2-1の相互認証部39と相互認証し、コンテンツプロバイダ2-1が、正当なプロバイダであることが確認した後、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、鍵サーバ14から供給された配送用鍵Kdをコンテンツプロバイダ2-1に送信する。なお、相互認証処理の詳細は、図41乃至図43を参照して後述する。

次に、ステップS32において、コンテンツプロバイダ2-1の暗号化部36は、EMDサービスセンタ1から送信された配送用鍵Kdを受信し、ステップS33において、記憶する。

このように、コンテンツプロバイダ2-1の暗号化部36が、配送用鍵Kdを記憶したとき、処理は終了し、図39のステップS12に進む。ここで、ステップS12以降の処理の説明の前に、図40のステップS31における相互認証処

理（なりすましがいないことを確認する処理）について、1つの共通鍵を用いる場合（図41）、2つの共通鍵を用いる場合（図42）、および公開鍵暗号を用いる場合（図43）を例として説明する。

図41は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS41において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する（乱数生成部35が生成するようにしてもよい）。ステップS42において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を、予め記憶している共通鍵Kcで暗号化する（暗号化部36で暗号化するようにしてもよい）。ステップS43において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

ステップS44において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kcで復号する。ステップS45において、EMDサービスセンタ1の相互認証部17は、32ビットの乱数R2を生成する。ステップS46において、EMDサービスセンタ1の相互認証部17は、復号した64ビットの乱数R1の下位32ビットを乱数R2で入れ替え、接続 $R1_H \parallel R2$ を生成する。なお、ここで $R1_H$ は、R1の上位nビットを表し、 $A \parallel B$ は、AとBの接続（nビットのAの下位に、mビットのBを結合して、 $(n+m)$ ビットとしたもの）を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R1_H \parallel R2$ を共通鍵Kcで暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R1_H \parallel R2$ をコンテンツプロバイダ2に送信する。

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R1_H \parallel R2$ を共通鍵Kcで復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R1_H \parallel R2$ の上位32ビット $R1_H$ を調べ、ステップS41で生成した、乱数R1の上位32ビット $R1_H$ と一致す

れば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 R_{1H} と、受信した R_{1H} が一致しないとき、処理は終了される。両者が一致するとき、ステップS51において、コンテンツプロバイダ2の相互認証部39は、32ビットの乱数 R_3 を生成する。ステップS52において、コンテンツプロバイダ2の相互認証部39は、受信して復号した $R_{1H} \parallel R_2$ から下位32ビットを取り出した乱数 R_2 を上位に設定し、生成した乱数 R_3 をその下位に設定し、接続 $R_2 \parallel R_3$ とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続 $R_2 \parallel R_3$ を共通鍵 K_c で暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続 $R_2 \parallel R_3$ をEMDサービスセンタ1の相互認証部17に送信する。

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続 $R_2 \parallel R_3$ を共通鍵 K_c で復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続 $R_2 \parallel R_3$ の上位32ビットを調べ、乱数 R_2 と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図42は、2つの共通鍵 K_{c1} 、 K_{c2} で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 R_1 を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数 R_1 を予め記憶している共通鍵 K_{c1} で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数 R_1 をEMDサービスセンタ1に送信する。

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数 R_1 を予め記憶している共通鍵 K_{c1} で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数 R_1 を予め記憶してい

る共通鍵 K_c2 で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数 $R2$ を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数 $R2$ を共通鍵 K_c2 で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数 $R1$ および乱数 $R2$ をコンテンツプロバイダ2の相互認証部39に送信する。

ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数 $R1$ および乱数 $R2$ を予め記憶している共通鍵 K_c2 で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数 $R1$ を調べ、ステップS61で生成した乱数 $R1$ （暗号化する前の乱数 $R1$ ）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数 $R2$ を共通鍵 K_c1 で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数 $R2$ をEMDサービスセンタ1に送信する。

ステップS73において、EMDサービスセンタ1の相互認証部17は、受信した乱数 $R2$ を共通鍵 K_c1 で復号する。ステップS74において、EMDサービスセンタ1の相互認証部17は、復号した乱数 $R2$ が、ステップS66で生成した乱数 $R2$ （暗号化する前の乱数 $R2$ ）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図43は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS81において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 $R1$ を生成する。ステップS82において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵 K_{pcp} を含む証明書（認証局から予め取得しておいたもの）

と、乱数 R_1 を EMD サービスセンタ 1 の相互認証部 17 に送信する。

ステップ S 8 3 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した証明書の署名（認証局の秘密鍵 K_{sca} で暗号化されている）を、予め取得しておいた認証局の公開鍵 K_{pca} で復号し、コンテンツプロバイダ 2 の公開鍵 K_{pcp} とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 K_{pcp} が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップ S 8 4 において、EMD サービスセンタ 1 の相互認証部 17 は、64 ビットの乱数 R_2 を生成する。ステップ S 8 5 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R_1 および乱数 R_2 の接続 $R_1 \parallel R_2$ を生成する。ステップ S 8 6 において、EMD サービスセンタ 1 の相互認証部 17 は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 K_{sesc} で暗号化する。ステップ S 8 7 において、EMD サービスセンタ 1 の相互認証部 17 は、接続 $R_1 \parallel R_2$ を、ステップ S 8 3 で取得したコンテンツプロバイダ 2 の公開鍵 K_{pcp} で暗号化する。ステップ S 8 8 において、EMD サービスセンタ 1 の相互認証部 17 は、秘密鍵 K_{sesc} で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 K_{pcp} で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 K_{pesc} を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

ステップS 8 9において、コンテンツプロバイダ2の相互認証部3 9は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 K_{pca} で復号し、正しければ証明書から公開鍵 K_{pesc} を取り出す。この場合の処理は、ステップS 8 3における場合と同様であるので、その説明は省略する。ステップS 9 0において、コンテンツプロバイダ2の相互認証部3 9は、EMDサービスセンタ1の秘密鍵 K_{sec} で暗号化されている接続 $R1 \parallel R2$ を、ステップS 8 9で取得した公開鍵 K_{pesc} で復号する。ステップS 9 1において、コンテンツプロバイダ2の相互認証部3 9は、自分自身の公開鍵 K_{pcp} で暗号化されている接続 $R1 \parallel R2$ を、自分自身の秘密鍵 K_{scp} で復号する。ステップS 9 2において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で復号された接続 $R1 \parallel R2$ と、ステップS 9 1で復号された接続 $R1 \parallel R2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップS 9 3において、コンテンツプロバイダ2の相互認証部3 9は、64ビットの乱数 $R3$ を生成する。ステップS 9 4において、コンテンツプロバイダ2の相互認証部3 9は、ステップS 9 0で取得した乱数 $R2$ および生成した乱数 $R3$ の接続 $R2 \parallel R3$ を生成する。ステップS 9 5において、コンテンツプロバイダ2の相互認証部3 9は、接続 $R2 \parallel R3$ を、ステップS 8 9で取得した公開鍵 K_{pesc} で暗号化する。ステップS 9 6において、コンテンツプロバイダ2の相互認証部3 9は、暗号化した接続 $R2 \parallel R3$ をEMDサービスセンタ1の相互認証部1 7に送信する。

ステップS 9 7において、EMDサービスセンタ1の相互認証部1 7は、暗号化された接続 $R2 \parallel R3$ を自分自身の秘密鍵 K_{sec} で復号する。ステップS 9 8において、EMDサービスセンタ1の相互認証部1 7は、復号した乱数 $R2$ が、ステップS 8 4で生成した乱数 $R2$ （暗号化する前の乱数 $R2$ ）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵 K_{temp} として利用される。

(6-2) コンテンツプロバイダからサービスプロバイダへのコンテンツの伝送
次に、図39のステップS12の処理について説明する。ステップS12においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2-1からサービスプロバイダ3-1に供給される処理が行われる。その処理の詳細は、図44のフローチャートに示されている。すなわち、ステップS201において、コンテンツプロバイダ2-1のウォータマーク付加部32は、コンテンツサーバ31からコンテンツAを読み出し、コンテンツプロバイダ2-1を示す所定のウォータマーク（電子透かし）を挿入し、圧縮部33に供給する。

ステップS202において、コンテンツプロバイダ2-1の圧縮部33は、ウォータマークが挿入されたコンテンツAをATRAC2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS203において、乱数発生部35は、コンテンツ鍵 K_{coA} となる乱数を発生させ、暗号化部34に供給する。

ステップS204において、コンテンツプロバイダ2-1の暗号化部34は、DESなどの所定の方式で、乱数発生部35で発生された乱数（コンテンツ鍵 K_{coA} ）を使用して、ウォータマークが挿入されて圧縮されたコンテンツAを暗号化する。次に、ステップS205において、暗号化部36は、DESなどの所定の方式で、EMDサービスセンタ1から供給された配送用鍵 K_d でコンテンツ鍵 K_{coA} を暗号化する。

ステップS206において、コンテンツプロバイダ2-1のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵 K_{coA} で暗号化されている）、コンテンツ鍵 K_{coA} （配送用鍵 K_d で暗号化されている）、およびポリシー記憶部37に記憶されている、コンテンツAに対応するUCPA, B（図12）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵 K_{scp} で暗号化する。これにより、図17に示した署名が作成される。

ステップS 2 0 7において、コンテンツプロバイダ2-1のセキュアコンテンツ作成部3 8は、コンテンツA（コンテンツ鍵K c o Aで暗号化されている）、コンテンツ鍵K c o A（配送用鍵K dで暗号化されている）、UCPA, B（図1 2）、およびステップS 2 0 6で生成した署名を含んだ、図1 7に示したコンテンツプロバイダセキュアコンテンツを作成する。

ステップS 2 0 8において、コンテンツプロバイダ2-1の相互認証部3 9は、サービスプロバイダ3-1の相互認証部4 5と相互認証する。この認証処理は、図4 1乃至図4 3を参照して説明した場合と同様であるので、その説明は省略する。ステップS 2 0 9において、コンテンツプロバイダ2-1のセキュアコンテンツ作成部3 8は、認証局から予め発行された証明書（図1 8）を、ステップS 2 0 7で作成したコンテンツプロバイダセキュアコンテンツに付して、サービスプロバイダ3-1に送信する。

このようにして、コンテンツプロバイダセキュアコンテンツが、サービスプロバイダ3-1に供給されたとき、処理は終了し、図3 9のステップS 1 3に進む。

（6-3）サービスプロバイダからレシーバへのコンテンツの伝送

ステップS 1 3において、サービスプロバイダセキュアコンテンツが、サービスプロバイダ3-1からユーザホームネットワーク5（レシーバ5 1）に供給される。この処理の詳細は、図4 5のフローチャートに示されている。すなわち、ステップS 2 2 1において、サービスプロバイダ3-1の値付け部4 2は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテンツに付された証明書（図1 8）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2-1の公開鍵K p c pを取り出す。証明書の署名の確認は、図4 3のステップS 8 3における処理と同様であるので、その説明は省略する。

ステップS 2 2 2において、サービスプロバイダ3-1の値付け部4 2は、コンテンツプロバイダ2-1から送信されたコンテンツプロバイダセキュアコンテンツの署名をコンテンツプロバイダ2-1の公開鍵K p c pで復号し、得られたハ

ッシュ値が、コンテンツ A (コンテンツ鍵 $K_{c o A}$ で暗号化されている)、コンテンツ鍵 $K_{c o A}$ (配送用鍵 K_d で暗号化されている)、および $U C P A, B$ の全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合 (改竄が発見された場合) は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップ S 2 2 3 に進む。

ステップ S 2 2 3 において、サービスプロバイダ 3-1 の値付け部 4 2 は、コンテンツプロバイダセキュアコンテナから、コンテンツ A (コンテンツ鍵 $K_{c o A}$ で暗号化されている)、コンテンツ鍵 $K_{c o A}$ (配送用鍵 K_d で暗号化されている)、および署名を取り出し、コンテンツサーバ 4 1 に供給する。コンテンツサーバ 4 1 は、それらを記憶する。値付け部 4 2 はまた $U C P A, B$ も、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部 4 4 に供給する。

ステップ S 2 2 4 において、サービスプロバイダ 3-1 の値付け部 4 2 は、取り出した $U C P A, B$ に基づいて、 $P T A-1, A-2$ (図 2 0)、および $P T B-1, B-2$ (図 2 2) を作成し、セキュアコンテナ作成部 4 4 に供給する。

ステップ S 2 2 5 において、サービスプロバイダ 3-1 のセキュアコンテナ作成部 4 4 は、コンテンツサーバ 4 1 から読み出したコンテンツ A (コンテンツ鍵 $K_{c o A}$ で暗号化されている)、コンテンツ鍵 $K_{c o A}$ (配送用鍵 K_d で暗号化されている)、およびコンテンツプロバイダ 2 の署名、値付け部 4 2 から供給された、 $U C P A, B$ 、および $P T A-1, A-2, B-1, B-2$ 、並びにその署名から、図 2 4 に示したサービスプロバイダセキュアコンテナを作成する。

ステップ S 2 2 6 において、サービスプロバイダ 3-1 の相互認証部 4 5 は、レシーバ 5 1 の相互認証モジュール 7 1 と相互認証する。この認証処理は、図 4 1 乃至図 4 3 を参照して説明した場合と同様であるので、その説明を省略する。

ステップ S 2 2 7 において、サービスプロバイダ 3-1 のセキュアコンテナ作

成部 4 4 は、ステップ S 2 2 5 で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ 3 - 1 の証明書（図 2 5）を付して、ユーザホームネットワーク 5 のレシーバ 5 1 に送信する。

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ 3 - 1 からレシーバ 5 1 に送信されたとき、処理は終了し、図 3 9 のステップ S 1 4 に進む。

（6 - 4）レシーバによるコンテンツの記録処理

ステップ S 1 4 において、サービスプロバイダ 3 - 1 から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク 5 のレシーバ 5 1 により受信される。この処理の詳細は、図 4 6 のフローチャートに示されている。すなわち、ステップ S 2 4 1 において、レシーバ 5 1 の相互認証モジュール 7 1 は、通信部 6 1 を介して、サービスプロバイダ 3 - 1 の相互認証部 4 5 と相互認証し、相互認証できたとき、通信部 6 1 は、相互認証したサービスプロバイダ 3 - 1 から、サービスプロバイダセキュアコンテナ（図 2 4）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップ S 2 4 2 に進む。

ステップ S 2 4 2 において、レシーバ 5 1 の通信部 6 1 は、ステップ S 2 4 1 で相互認証したサービスプロバイダ 3 - 1 から、公開鍵証明書を受信する。

ステップ S 2 4 3 において、レシーバ 5 1 の復号／暗号化モジュール 7 4 は、ステップ S 2 4 1 で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップ S 2 4 4 に進む。

ステップ S 2 4 4 において、UCP および PT が選択され、かつ、その利用内容および価格内容が選択される。具体的には、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている基準情報 5 1（図 3 2）に基づいて、利用条件を満たす UCP と価格条件を満たす PT が選択される。この例の場合、レシーバ 5 1 の基準情

報51の「利用ポイント情報」には、図33に示したように、コンテンツプロバイダ2-1のコンテンツ利用ポイントが222ポイントであるとされている。すなわち、この基準情報51によれば、コンテンツAに対応して設定されたUCPA、Bのうち、「利用条件10」の「ユーザ条件10」が”200ポイント以上”とされているUCPA（図12A）が選択される。また、基準情報51の「決済ユーザ情報」には、ユーザFは男性とされているので、PTA-1（図20A）の「価格条件10」に設定された条件を満たす。その結果、UCPAに対応して作成されたPTA-1、PTA-2のうち、PTA-1が選択される。

その後、このようにして選択されたUCPAおよびPTA-1の内容が、表示制御部67を介して、図示せぬ表示部に表示される。そこで、ユーザFは、その表示を参照して（例えば、利用したい利用形式と、その価格を比較検討して）、UCPAの所定の「利用内容」を選択するための操作を、図示せず操作部に対して行う。これにより、入力制御部68を介して、選択されたUCPAの利用内容のIDおよびPTA-1のIDがSAM62に出力される。なお、この例の場合、UCPAの利用内容11（PTA-1の価格内容11）が選択されたものとする。

ステップS245において、レシーバ51のSAM62の課金処理モジュール72は、ステップS244で選択された、UCPAの「利用内容11」とPTA-1に基づいて、UCSA（図28）および課金情報A（図30）を作成する。すなわち、この場合、コンテンツAは、料金が2000円で買い取り再生される。

ステップS246において、サービスプロバイダセキュアコンテナ（図24）に含まれる、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、UCPA、PTA-1、A-2、およびコンテンツプロバイダ2の署名が取り出され、HDD52に出力され、記憶される。ステップS247において、復号/暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）を、記憶モジ

ジュール73に記憶されている配送用鍵K_dで復号する。

ステップS248において、復号／暗号化ユニット74の暗号化ユニット93は、ステップS247で復号されたコンテンツ鍵K_{coA}を、記憶モジュール73に記憶されている保存用鍵K_{save}で暗号化する。

ステップS249において、レシーバ51のデータ検査モジュール75は、ステップS248で保存用鍵K_{save}で暗号化されたコンテンツ鍵K_{coA}、およびステップS245で作成されたUCSAが対応して記憶される、外部記憶部63の利用情報記憶部63A（図29）の空き領域を有するブロックBPを検出する。この例の場合、利用情報記憶部63AのブロックBP-1が検出される。なお、図29の利用情報記憶部63Aにおいて、そのブロックBP-1の利用情報用メモリ領域RP-3にコンテンツ鍵K_{coA}およびUCSAが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、空いることを示す所定の初期情報が記憶されている。

ステップS250において、レシーバ51のデータ検査モジュール75は、ステップS249で検出したブロックBP-1のデータ（利用情報用メモリ領域RP-1乃至RP-Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップS251において、データ検査モジュール75は、ステップS250で得られたハッシュ値と、記憶モジュール73に記憶されているブロックBP-1に対応する検査値HP-1（図31）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックBP-1のデータは改竄されていないので、ステップS252に進む。

ステップS252において、レシーバ51のSAM62は、利用情報（ステップS248で、保存用鍵K_{save}で暗号化されたコンテンツ鍵K_{coA}、およびステップS245で作成されたUCSA）を、外部記憶部63のブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。

ステップS253において、レシーバ51のデータ検査モジュール75は、ステップS252で利用情報が記憶された利用情報用メモリ領域RP-3が属する

、利用情報記憶部 6 3 A のブロック B P - 1 に記憶されている全てのデータにハッシュ関数を適用してハッシュ値を算出し、ステップ S 2 5 4 において、記憶モジュール 7 3 に記憶されている検査値 H P - 1 に上書きする。ステップ S 2 5 5 において、課金処理モジュール 7 2 は、ステップ S 2 4 5 で作成した課金情報 A を記憶モジュール 7 3 に記憶させ、処理は終了する。

ステップ S 2 5 1 において、算出されたハッシュ値と検査値 H P - 1 とが一致しないと判定された場合、ブロック B P - 1 のデータは改竄されているので、手続きは、ステップ S 2 5 6 に進み、データ検査モジュール 7 5 は、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック B P を調べたか否かを判定し、外部記憶部 6 3 の全てのブロック B P を調べていないと判定した場合、ステップ S 2 5 7 に進み、利用情報記憶部 6 3 A の、空きを有する他のブロック B P を検索し、ステップ S 2 5 0 に戻り、それ以降の処理が実行される。

ステップ S 2 5 6 において、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック B P が調べられたと判定された場合、利用情報を記憶できるブロック B P (利用情報用メモリ領域 R P) は存在しないので、処理は終了する。

このように、サービスプロバイダセキュアコンテナが、レシーバ 5 1 により受信されると、処理は終了し、図 3 9 のステップ S 1 5 に進む。

(6-5) コンテンツの再生処理

ステップ S 1 5 において、供給されたコンテンツ A が、レシーバ 5 1 において利用される。なお、この例の場合選択された U C P A の利用内容 1 1 によれば、コンテンツ A は、再生して利用される。そこで、ここでは、コンテンツ A の再生処理について説明する。この再生処理の詳細は、図 4 7 のフローチャートに示されている。

ステップ S 2 6 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、図 4 6 のステップ S 2 5 2 で、コンテンツ鍵 K c o A (保存用鍵 K s a v e で暗号化されている) および U C S A が記憶された利用情報用メモリ領域 R P - 3 が属する、外部記憶部 6 3 の利用情報記憶部 6 3 A のブロック B P - 1 のデータにハ

ッシュ関数を適用してハッシュ値を算出する。

ステップS 2 6 2において、レシーバ5 1のデータ検査モジュール7 5は、ステップS 2 6 1において算出したハッシュ値が、図4 6のステップS 2 5 3で算出し、ステップS 2 5 4で記憶モジュール7 3に記憶させたハッシュ値（検査値HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロックBP-1のデータは改竄されていないので、ステップS 2 6 3に進む。

ステップS 2 6 3において、UCSA（図2 8）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツAが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。現在の時刻がその範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が0回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が0回であるとき、利用不可と判定される。

なお、UCSAの「利用内容」の「形式」は、「買い取り再生」とされているので、この場合、コンテンツAは、買い取られ、制限なしに再生される。すなわち、UCSAの「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップS 2 6 3において、コンテンツAが利用可能であると判定され、ステップS 2 6 4に進む。

ステップS 2 6 4において、レシーバ5 1の課金モジュール7 2は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、そ

の「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

次に、ステップS 2 6 5において、レシーバ5 1のSAM 6 2は、ステップS 2 6 4で更新されたUCSA（この例の場合には、実際は、更新されていない）を、外部記憶部6 3の利用情報記憶部6 3 AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS 2 6 6において、データ検査モジュール7 5は、ステップS 2 6 5でUCSAが記憶された、外部記憶部6 3の利用情報記憶部6 3 AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール7 3に記憶されている検査値HP-1に上書きする。

ステップS 2 6 7において、SAM 6 2の相互認証モジュール7 1と、伸張部6 4の相互認証モジュール1 0 1は、相互認証し、SAM 6 2および伸張部6 4は、一時鍵K t e m pを共有する。この認証処理は、図4 1乃至図4 3を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R 1、R 2、R 3、またはその組み合わせが、一時鍵K t e m pとして用いられる。

ステップS 2 6 8において、復号／暗号化モジュール7 4の復号ユニット9 1は、図4 6のステップS 2 5 2で外部記憶部6 3の利用情報記憶部6 3 AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵K c o A（保存用鍵K s a v eで暗号化されている）を、記憶モジュール7 3に記憶された保存用鍵K s a v eで復号する。

次に、ステップS 2 6 9において、復号／暗号化モジュール7 4の暗号化ユニット9 3は、復号されたコンテンツ鍵K c o Aを一時鍵K t e m pで暗号化する。ステップS 2 7 0において、SAM 6 2は、一時鍵K t e m pで暗号化されたコンテンツ鍵K c o Aを伸張部6 4に送信する。

ステップS 2 7 1において、伸張部6 4の復号モジュール1 0 2は、コンテンツ鍵K c o Aを一時鍵K t e m pで復号する。ステップS 2 7 2において、伸張

部64は、インタフェース66を介して、HDD52に記録されたコンテンツA（コンテンツ鍵Kc oで暗号化されている）を受け取る。ステップS273において、伸張部64の復号モジュール103は、コンテンツA（コンテンツ鍵Kc oで暗号化されている）をコンテンツ鍵Kc o Aで復号する。

ステップS274において、伸張部64の伸張モジュール104は、復号されたコンテンツAをATRAC2などの所定の方式で伸張する。ステップS275において、伸張部64のウォータマーク付加モジュール105は、伸張されたコンテンツAにレシーバ51を特定する所定のウォータマーク（電子透かし）を挿入する。ステップS276において、コンテンツAは、図示せぬスピーカなどに出力され、再生される。その後、処理は終了する。

ステップS262において、ステップS261において算出されたハッシュ値が、レシーバ51の記憶モジュール73に記憶された検査値HP-1と一致しないと判定された場合、またはステップS263において、コンテンツが利用不可と判定された場合、ステップS277において、SAM62は、表示制御部67を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

このようにして、レシーバ51において、コンテンツAが再生（利用）されたとき、処理は終了し、図39の処理も終了する。

なお、以上においては、コンテンツAが、レシーバ51において利用（購入）される場合を例として説明したが、レシーバ201も、レシーバ51と同様に、コンテンツAを利用することができる。ただし、レシーバ201の基準情報201の「利用ポイント情報」には、図38に示したように、コンテンツプロバイダ2-1のコンテンツ利用ポイントが23ポイントとされているので、UCPAの「利用条件10」の「ユーザ条件10」の条件を満たさない。すなわち、この場合、UCPAは選択されず、UCPBが選択される。

次に、PTが選択されるが、この場合、UCPBが選択されているので、UCPBに対応するPTB-1、B-2（図22）のうちのいずれかが選択される。

P T B - 1 の「価格条件 3 0」は、機器が従機器であることが条件とされ、また P T B - 2 の「価格条件 4 0」は、主機器であることが条件とされている。すなわち、主機器であるレシーバ 2 0 1 においては、P T B - 2 が選択される。このように、機器およびそのユーザに設定された各種条件に基づいて、U C P、U C P の利用内容、および P T の選択範囲が決定される。

また、以上においては、U C P の「利用条件」または P T の「価格条件」の「ユーザ条件」を、ユーザの性別や年齢に関する条件とする場合を例として説明したが、例えば、ユーザの住んでいる地域や誕生日などを条件とすることもできる。なお、この場合、図 1 5 A のサービスコードの 0 3 0 0 h 乃至 7 F F F h のコート値に、それらの条件の意味を設定する。

(6 - 6) 決済処理

次に、レシーバ 5 1 の課金が決済される場合の処理手順を、図 4 8 のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を超えた場合、または配送用鍵 K d のバージョンが古くなり、例えば、図 4 6 のステップ S 2 4 7 で、コンテンツ鍵 K c o （配送用鍵 K d で暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

すなわち、ステップ S 3 0 1 において、レシーバ 5 1 と EMD サービスセンタ 1 との相互認証が行われる。この相互認証は、図 4 1 乃至図 4 3 を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップ S 3 0 2 において、レシーバ 5 1 の S A M 6 2 は、EMD サービスセンタ 1 のユーザ管理部 1 8 に証明書を送信する。ステップ S 3 0 3 において、レシーバ 5 1 の S A M 6 2 は、記憶モジュール 7 3 に記憶されている課金情報を、ステップ S 3 0 1 で EMD サービスセンタ 1 と共有した一時鍵 K t e m p で暗号化し、配送用鍵 K d のバージョン、HDD 5 2 に記憶されている U C P および P T、並びに登録リストとともに、EMD サービスセンタ 1 に送信する。

ステップS 3 0 4において、EMDサービスセンタ1のユーザ管理部18は、ステップS 3 0 3で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

ステップS 3 0 5において、EMDサービスセンタ1の課金請求部19は、ステップS 3 0 3で受信された課金情報を解析し、ユーザ（例えば、ユーザF）の支払い金額を算出する処理等を行う。次に、ステップS 3 0 6において、ユーザ管理部18は、ステップS 3 0 5における処理により、決済が成功したか否かを確認する。

次に、ステップS 3 0 7において、EMDサービスセンタ1のユーザ管理部18は、ステップS 3 0 4における確認結果、およびステップS 3 0 6における確認結果に基づいて、レシーバ51の登録条件を設定し、それに署名を付して、レシーバ51の登録リストを作成する。

例えば、ステップS 3 0 4で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS 3 0 6で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップS 3 0 8に進み、EMDサービスセンタ1のユーザ管理部18は、最新バージョンの配送用鍵K d（3ヶ月分の最新バージョンの配送用鍵K d）を一時鍵K t e m pで暗号化し、ステップS 3 0 7で作成された登録リストとともにレシーバ51に送信する。

ステップS 3 0 9において、レシーバ51のSAM62は、EMDサービスセンタ1から送信された配送用鍵K dおよび登録リストを、通信部61を介して受信し、復号した後、記憶モジュール73に記憶させる。このとき、記憶モジュール

ル 7 3 に記憶されていた課金情報は消去され、登録リストおよび配送用鍵 K d が更新される。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

上述の本発明の実施の形態のコンテンツプロバイダは、第 1 の情報に対応させて、利用条件および利用内容を含む第 2 の情報を記憶し、第 1 の情報に対応させて第 2 の情報を所定の機器に送信するようにしたので、利用条件に応じた第 1 の情報の配布を行うことが可能になる。

また、本発明の実施の形態のサービスプロバイダは、第 1 の情報の利用条件および利用内容を含む第 2 の情報に対応して、第 1 の情報の価格条件および価格内容を含む第 3 の情報を作成するようにし、第 1 の情報に対応させて第 2 の情報および第 3 の情報を、所定の機器に送信するようにしたので、条件に応じた価格で第 1 の情報を配布することが可能になる。

また、本発明の実施の形態のレシーバは、基準情報に対応して選択した利用条件に対応する利用内容に従って、コンテンツを利用し、基準情報に対応して選択した価格条件に対応する価格内容に従って、コンテンツの利用に対して、課金処理を実行するようにしたので、変化に富んだサービスを受けることができる。

産業上の利用の可能性

本発明は、音楽データ、動画像データ、静止画像データ、文書データ、プログラムデータなどの情報を暗号化し、配信する情報処理システムに適応できる。

請 求 の 範 囲

1. 暗号化されている第1の情報を保持する保持手段と、

上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報を、上記第1の情報に対応させて記憶する記憶手段と、

上記保持手段により保持されている暗号化されている上記第1の情報と、上記記憶手段により記憶されている上記第2の情報を所定の機器に送信する送信手段と

を具備する情報処理装置。

2. 暗号化されている第1の情報を保持する保持ステップと、

上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報を、上記第1の情報に対応させて記憶する記憶ステップと、

上記保持ステップで保持された暗号化されている上記第1の情報と、上記記憶ステップで記憶された上記第2の情報を所定の機器に送信する送信ステップと

を具備する情報処理方法。

3. 暗号化されている第1の情報を保持する保持ステップと、

上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報を、上記第1の情報に対応させて記憶する記憶ステップと、

上記保持ステップで保持された暗号化されている上記第1の情報と、上記記憶ステップで記憶された上記第2の情報を所定の機器に送信する送信ステップと

を具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

4. 所定のプロバイダから送信されてくる、暗号化されている第1の情報、および上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報を受信する受信手段と、

上記受信手段により受信された上記第2の情報に対応して、上記第1の情報の価格条件と上記価格条件に対応する価格内容を含む第3の情報を作成する作成手段と、

上記受信手段により受信された暗号化されている上記第1の情報および上記第2の情報、並びに上記作成手段により作成された上記第3の情報を、所定の機器に送信する送信手段と

を具備する情報処理装置。

5. 所定のプロバイダから送信されてくる、暗号化されている第1の情報、および上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、

上記受信ステップで受信された上記第2の情報に対応して、上記第1の情報の価格条件と上記価格条件に対応する価格内容を含む第3の情報を作成する作成ステップと、

上記受信ステップで受信された暗号化されている上記第1の情報および上記第2の情報、並びに上記作成ステップで作成された上記第3の情報を、所定の機器に送信する送信ステップと

を具備する情報処理方法。

6. 所定のプロバイダから送信されてくる、暗号化されている第1の情報、および上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報を受信する受信ステップと、

上記受信ステップで受信された上記第2の情報に対応して、上記第1の情報の価格条件と上記価格条件に対応する価格内容を含む第3の情報を作成する作成ス

テップと、

上記受信ステップで受信された暗号化されている上記第 1 の情報および上記第 2 の情報、並びに上記作成ステップで作成された上記第 3 の情報を、所定の機器に送信する送信ステップと

を具備する処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

7. 所定の基準情報を記憶する記憶手段と、

所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、上記第 1 の情報の利用条件と上記利用条件に対応する利用内容を含む第 2 の情報、および上記第 1 の情報の価格条件と上記価格条件に対応する価格内容を含む第 3 の情報を受信する受信手段と、

上記記憶手段に記憶されている上記基準情報に対応する、上記受信手段により受信された上記第 2 の情報の上記利用条件を選択する利用条件選択手段と、

上記記憶手段に記憶されている上記基準情報に対応する、上記受信手段により受信された上記第 3 の情報の上記価格条件を選択する価格条件選択手段と、

上記利用条件選択手段により選択された上記利用条件に対応する上記利用内容に従って、暗号化されている上記第 1 の情報を復号して、利用する利用手段と、

上記価格条件選択手段により選択された上記価格条件に対応する上記価格内容に従って、利用手段による利用に対する課金処理を実行する実行手段と

を具備する情報処理装置。

8. 所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第 1 の情報、上記第 1 の情報の利用条件と上記利用条件に対応する利用内容を含む第 2 の情報、および上記第 1 の情報の価格条件と上記価格条件に対応する価格内容を含む第 3 の情報を受信する受信ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第2の情報の上記利用条件を選択する利用条件選択ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第3の情報の上記価格条件を選択する価格条件選択ステップと、

上記利用条件選択ステップで選択された上記利用条件に対応する上記利用内容に従って、暗号化されている上記第1の情報を復号して、利用する利用ステップと、

上記価格条件選択ステップで選択された上記価格条件に対応する上記価格内容に従って、上記利用ステップでの利用に対する課金処理を実行する実行ステップと

を具備する情報処理方法。

9. 所定の基準情報を記憶する記憶ステップと、

所定のプロバイダから送信されてくる、暗号化されている第1の情報、上記第1の情報の利用条件と上記利用条件に対応する利用内容を含む第2の情報、および上記第1の情報の価格条件と上記価格条件に対応する価格内容を含む第3の情報を受信する受信ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第2の情報の上記利用条件を選択する利用条件選択ステップと、

上記記憶ステップで記憶された上記基準情報に対応する、上記受信ステップで受信された上記第3の情報の上記価格条件を選択する価格条件選択ステップと、

上記利用条件選択ステップで選択された上記利用条件に対応する上記利用内容に従って、暗号化されている上記第1の情報を復号して、利用する利用ステップと、

上記価格条件選択ステップで選択された上記価格条件に対応する上記価格内容に従って、上記利用ステップでの利用に対する課金処理を実行する実行ステップと

を含む処理を情報処理装置に実行させるコンピュータが読み取り可能なプログラムを提供する提供媒体。

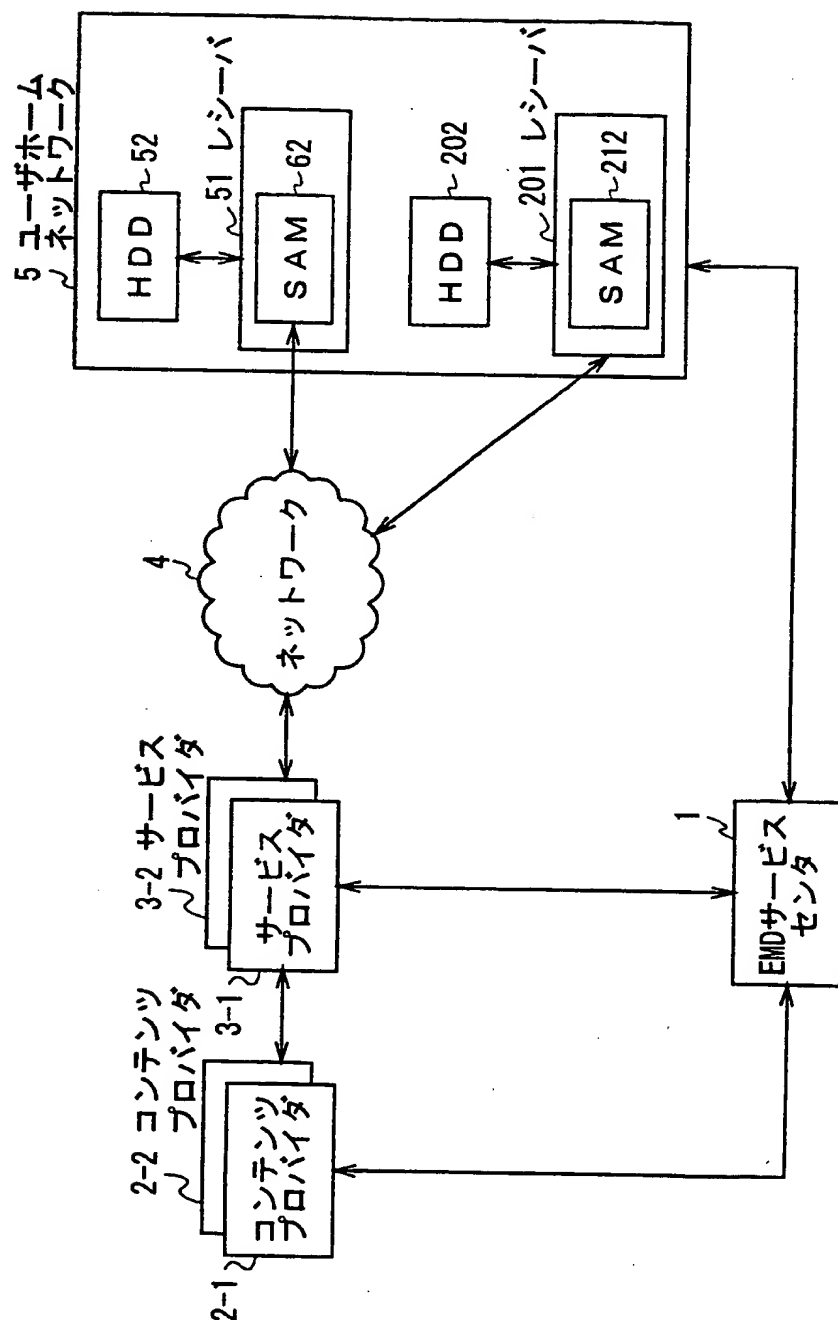


図 1

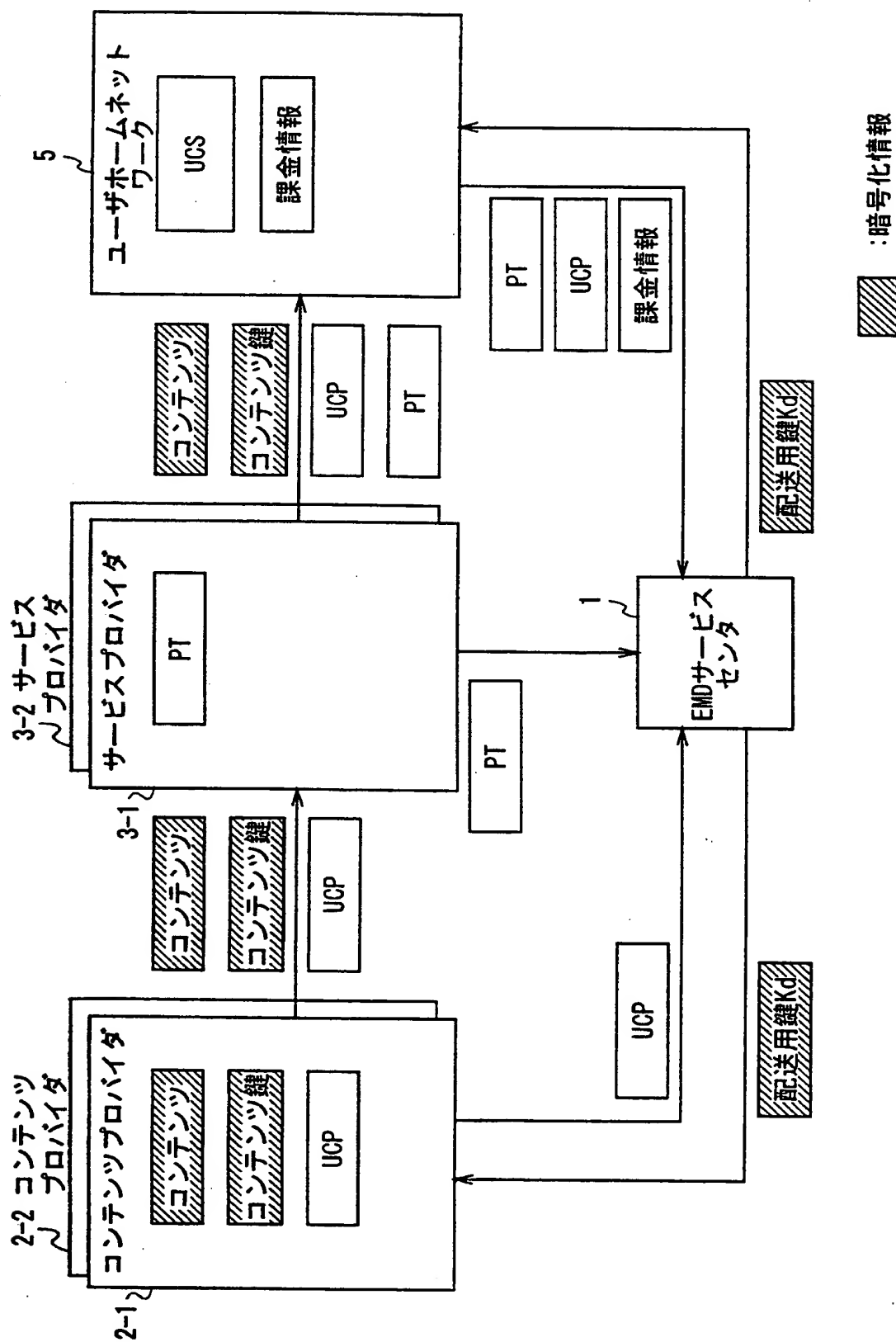
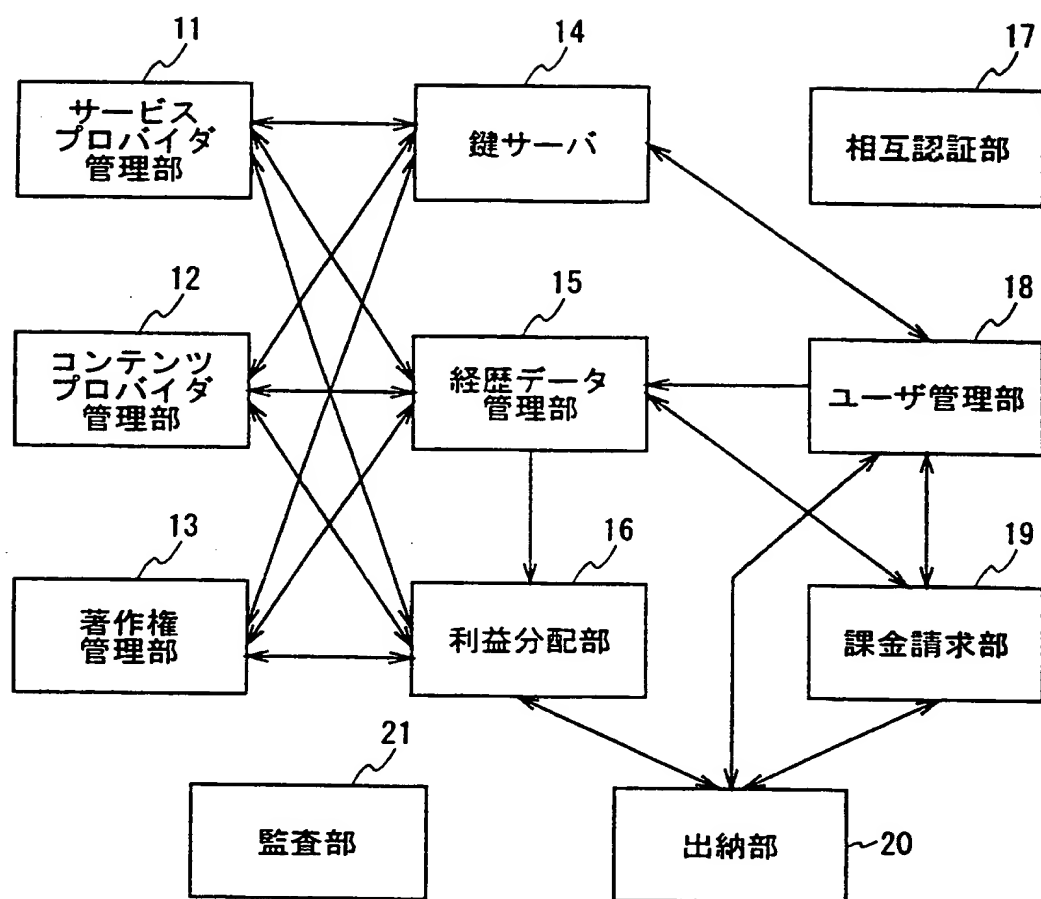


図 2



EMDサービスセンタ 1

図 3

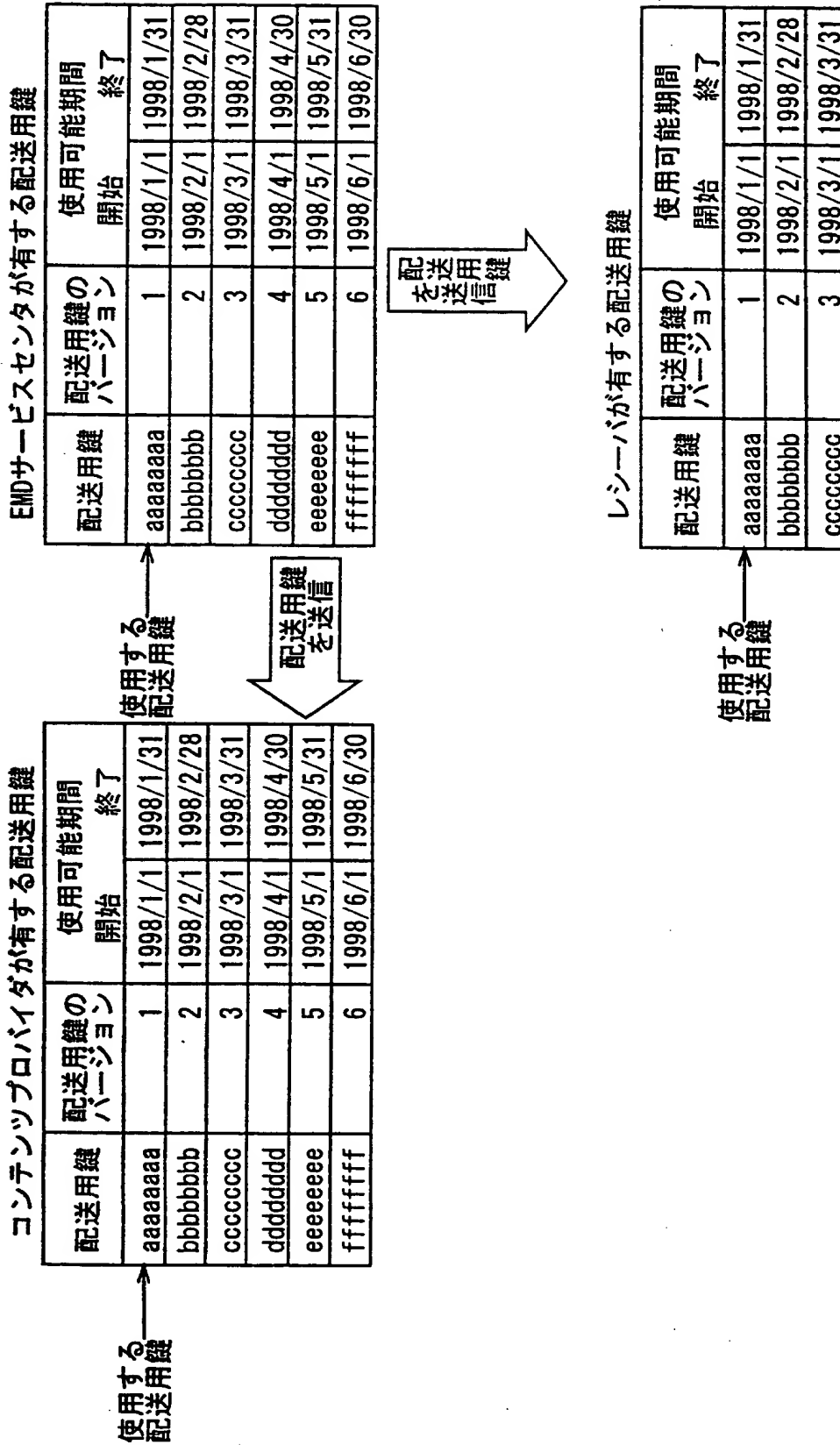


図 4

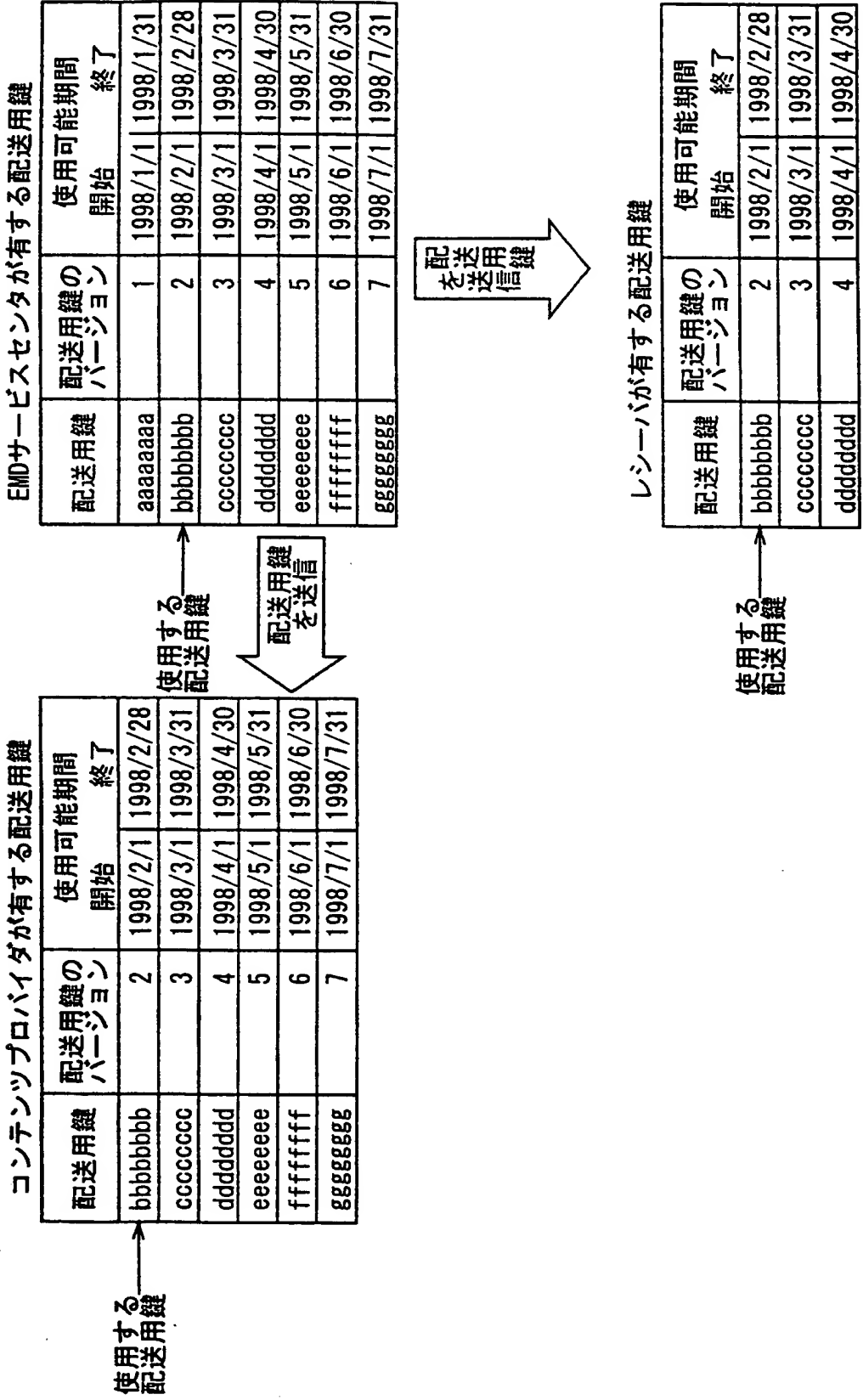


図 5

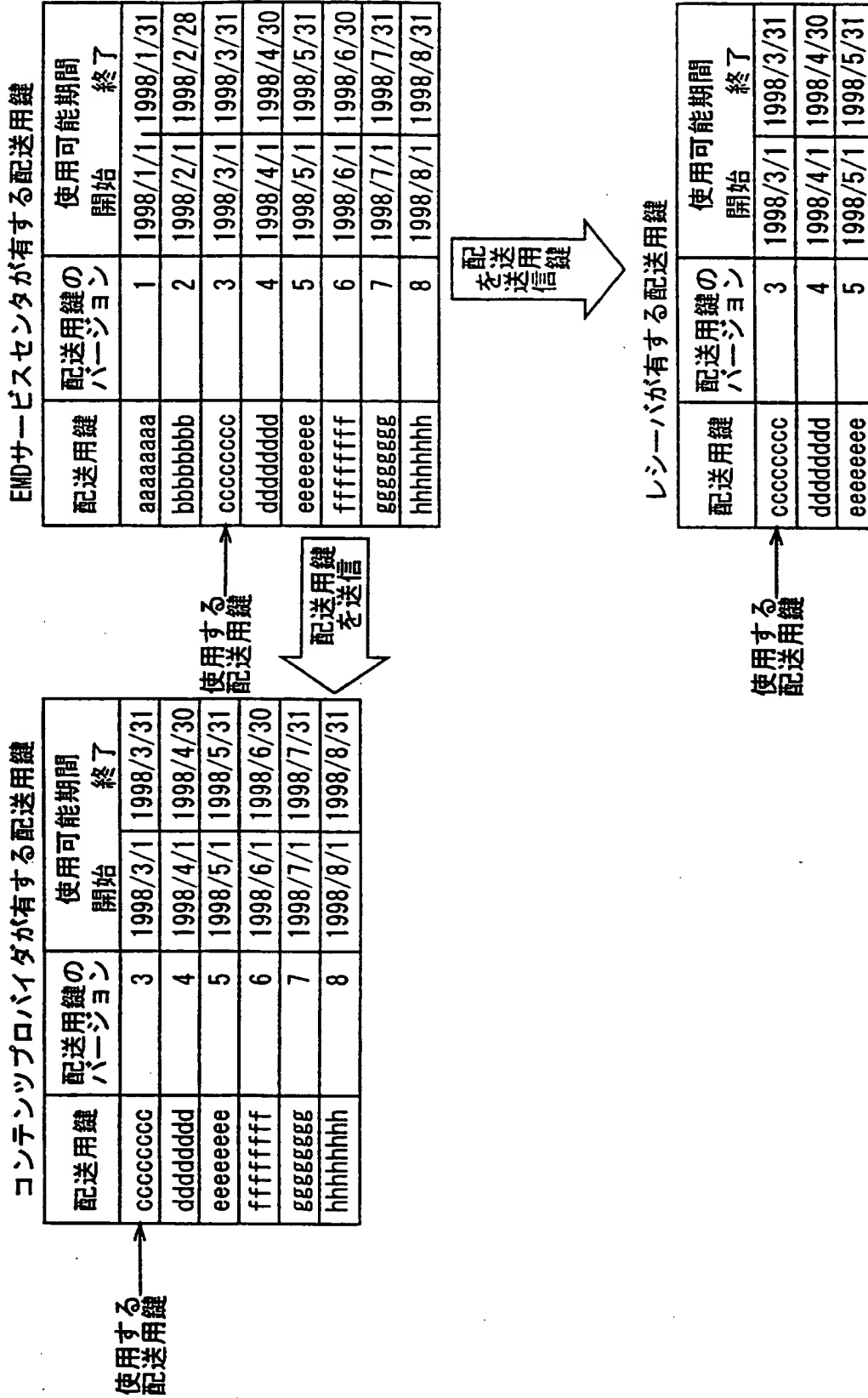


図 6

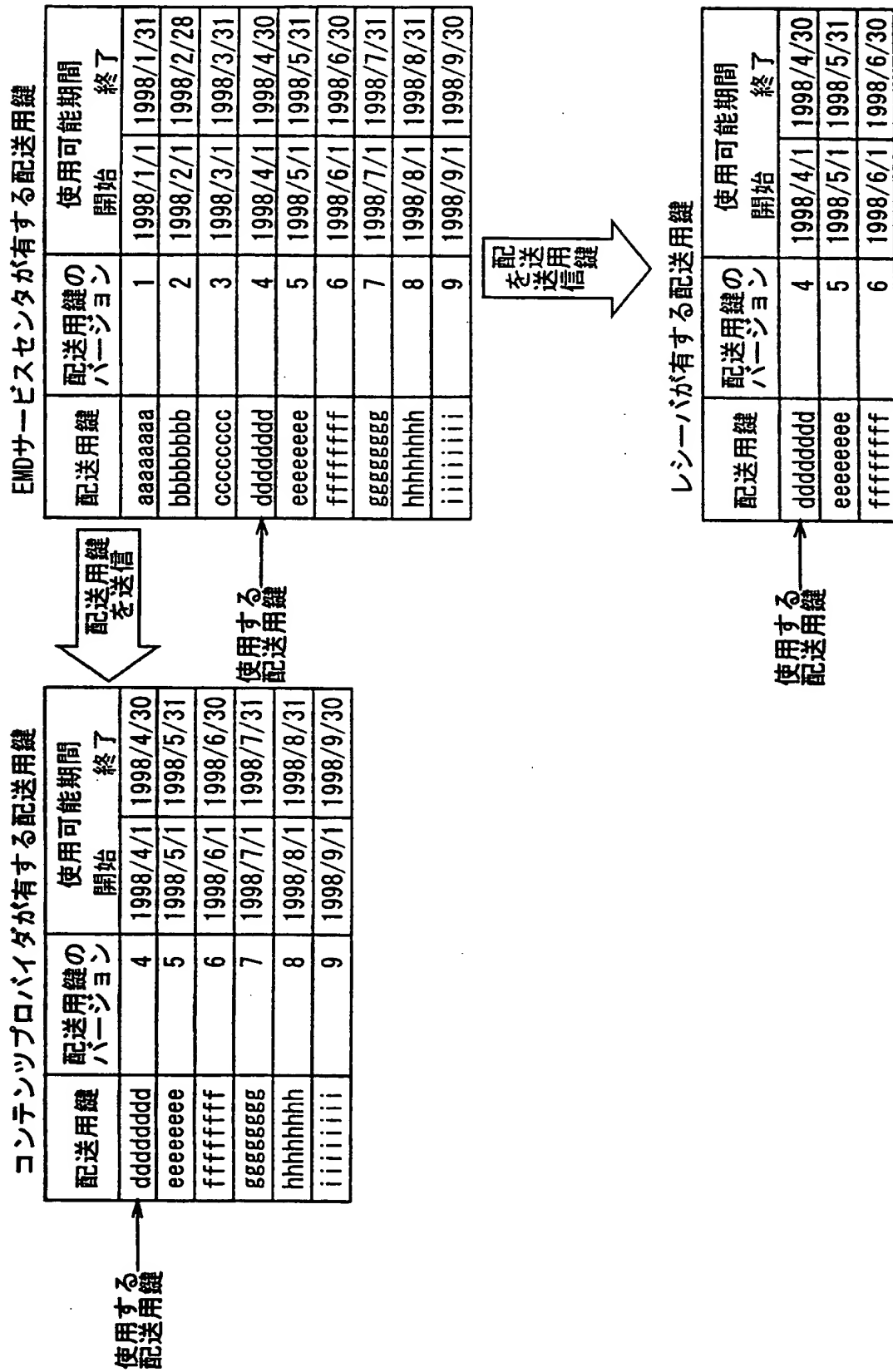


図 7

配送用鍵	配送用鍵の バージョン	使用可能期間 開始 終了
aaaaaaaa	1	1998/1/1 1998/1/31

仮配送用鍵Kd

図 8

SAMのID		SAM62のID	SAM212のID
機器番号		レシパ 51の機器番号 (100番)	レシパ 201の機器番号 (100番)
決済ID		ユーザFの決済ID	ユーザAの決済ID
決済 ユーザ 情報	氏名	ユーザFの氏名	ユーザAの氏名
	住所	ユーザFの住所	ユーザAの住所
	電話番号	ユーザFの電話番号	ユーザAの電話番号
	決済機関情報	ユーザFの決済情報	ユーザAの決済情報
	生年月日	ユーザFの生年月日	ユーザAの生年月日
	年齢	ユーザFの年齢	ユーザAの年齢
	性別	ユーザFの性別(男)	ユーザAの性別(女)
	ユーザのID	ユーザFのID	ユーザAのID
	パスワード	ユーザFのパスワード	ユーザAのパスワード
従属 ユーザ 情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
利用ポイント情報		レシパ 51の利用 ポイント情報	レシパ 201の利用 ポイント情報

システム登録情報

図 9

A

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	222ポイント
	コンテンツプロバイダ2-2	123ポイント
	サービスプロバイダ3-1	345ポイント
	サービスプロバイダ3-2	0ポイント

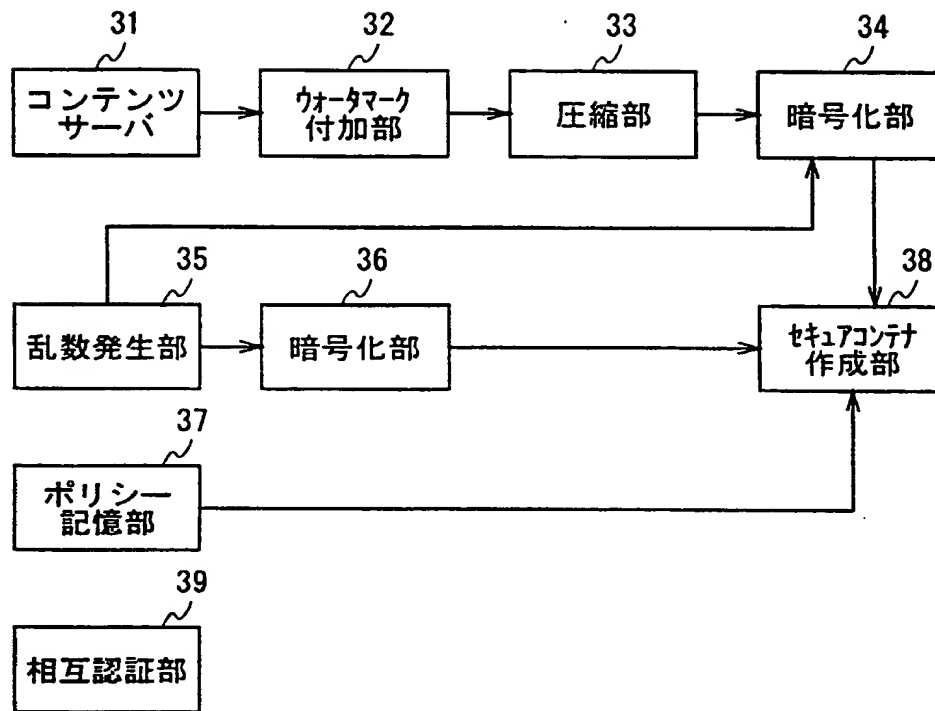
利用ポイント情報

B

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	23ポイント
	コンテンツプロバイダ2-2	22ポイント
	サービスプロバイダ3-1	40ポイント
	サービスプロバイダ3-2	5ポイント

利用ポイント情報

図 10



コンテンツプロバイダ 2-1

コンテンツのID	コンテンツのID	コンテンツAのID
コンテンツIDのID		コンテンツIDのID 2-1のID
UCPのID	UCPのID	UCPBのID
UCPの有効期限	UCPの有効期限	UCPBの有効期限
利用条件 20	ユーザ条件20	200ポイント より少ない
	機器条件20	条件なし
	ID 21	利用内容21のID
利用内容 21	形式21	Pay Per Play 4
	バージョン21	再生4回
	管理移動 許可情報21	不可
利用内容 22	ID 22	利用内容22のID
	形式22	Pay Per Copy 2
	バージョン22	複製2回
	管理移動 許可情報22	不可

UCPB

B

コンテンツのID	コンテンツAのID		
コンテンツIDのID	コンテンツIDのID 2-1のID		
UCPのID	UCPAのID		
UCPの有効期限	UCPAの有効期限		
利用条件 10	ユーザ条件10	200ポイント以上	
	機器条件10	条件なし	
利用内容 11	ID 11	利用内容11のID	
	形式11	買い取り再生	
	バージョン11	××××	
	管理移動許可情報11	可	
	ID 12	利用内容12のID	
利用内容 12	形式12	第1世代複製	
	バージョン12	××××	
	管理移動許可情報12	不可	
	ID 13	利用内容13のID	
利用内容 13	形式13	期間制限再生	
	バージョン13	××××	
	管理移動許可情報13	不可	
	ID 14	利用内容14のID	
利用内容 14	形式14	Pay Per Copy 5	
	バージョン14	複製5回	
	管理移動許可情報14	不可	

UCPA

図 1 2

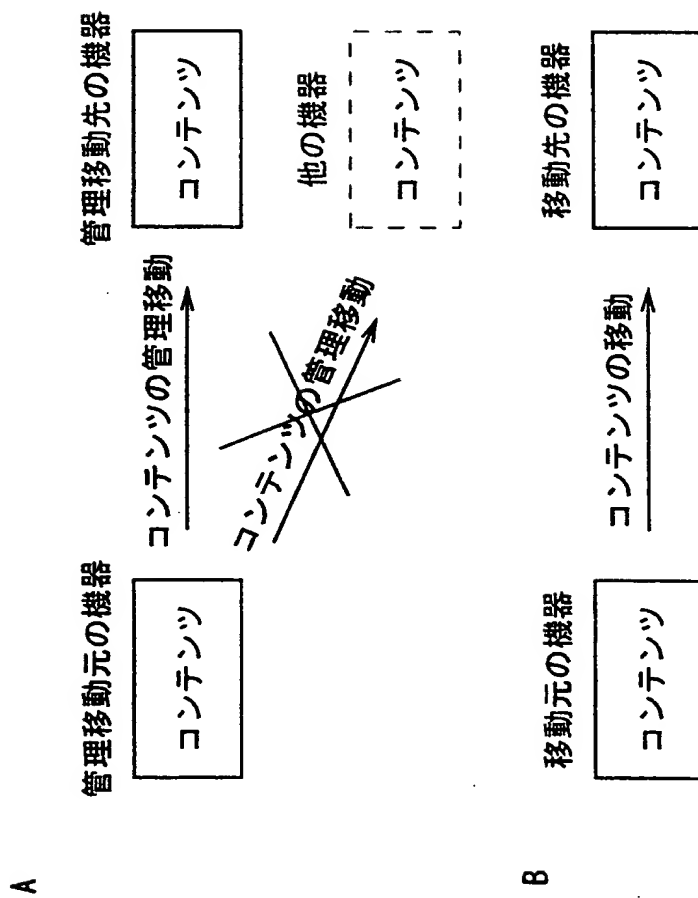


図 13

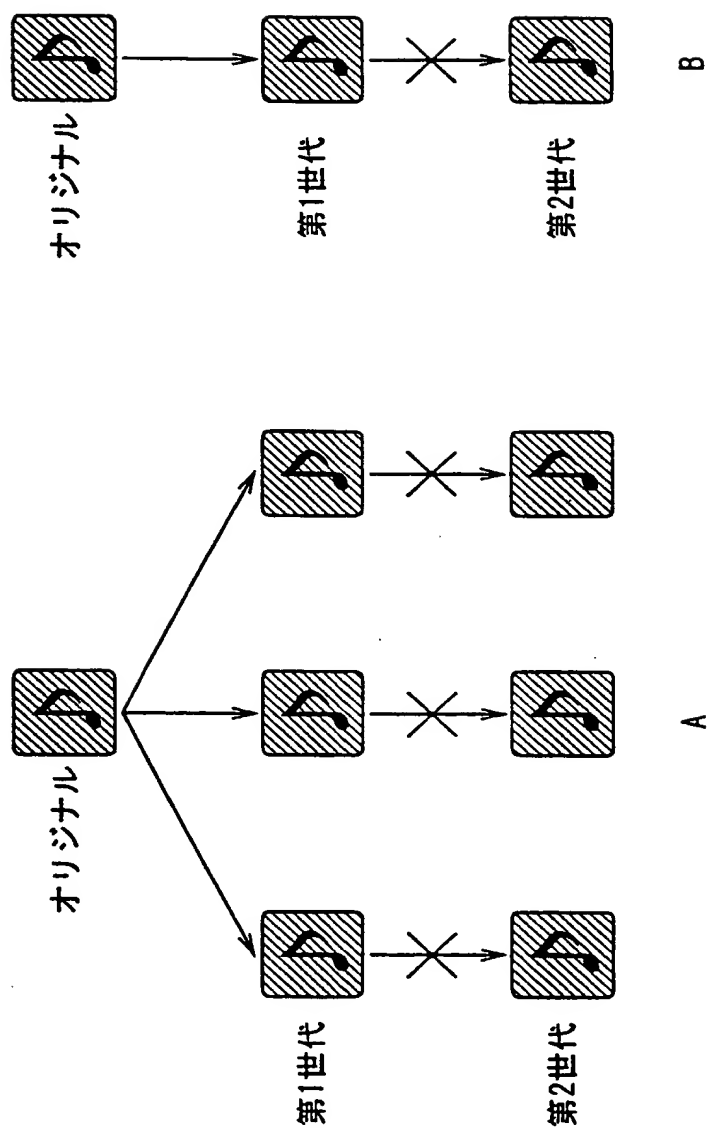


図 14

A

サービスコード	意味
0000h	条件なし
0001h乃至00FFh	機器に関し条件有り
0100h乃至01FFh	性別条件あり
0200h乃至02FFh	年令条件あり
0300h乃至7FFFh	その他の条件あり
8000h乃至FFFFh	利用ポイントに関し条件有り

B

コンディションコード	意味
00h	無条件
01h	=
02h	≠
03h	< (より小さい)
04h	> (より大きい)
05h	≤ (以下)
06h	≥ (以上)
07h乃至FFh	空き

図 1 5

A

ユーザ条件 10	サービスコード	ハッシュコード	コンディションコード
	80 × × h	0000C8h	06h
機器条件 10	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

UCPAの利用条件 10

B

ユーザ条件 20	サービスコード	ハッシュコード	コンディションコード
	80 × × h	0000C8h	03h
機器条件 20	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

UCPBの利用条件 20

図 16

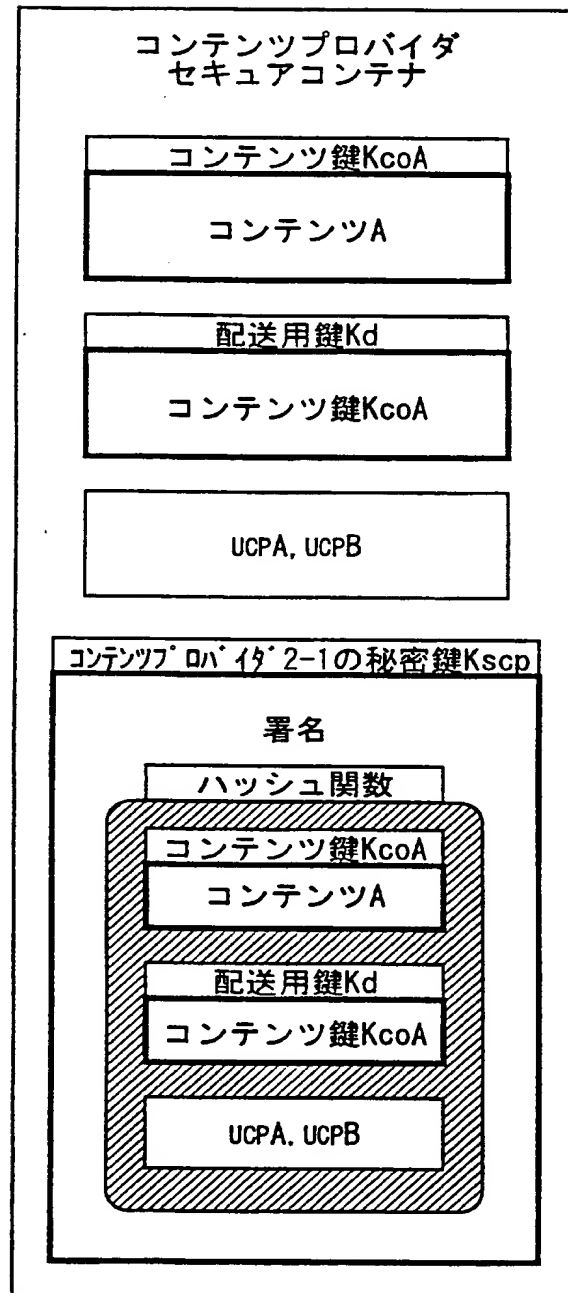


図 17

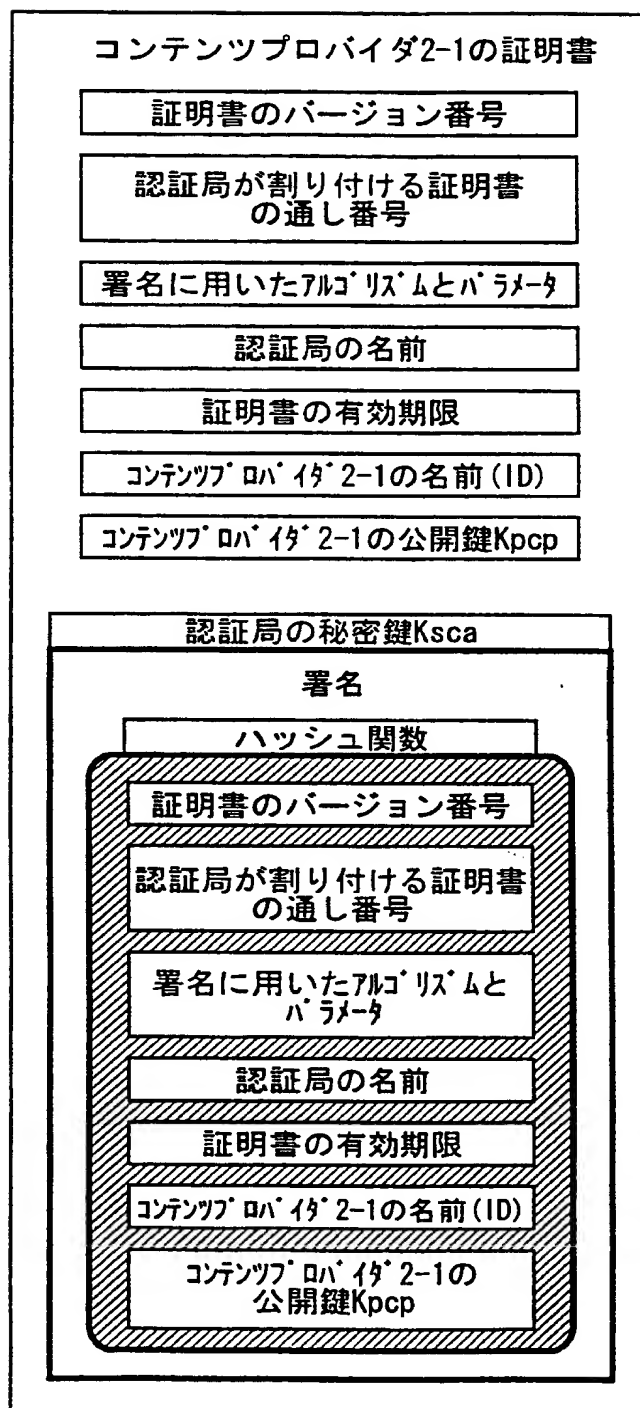
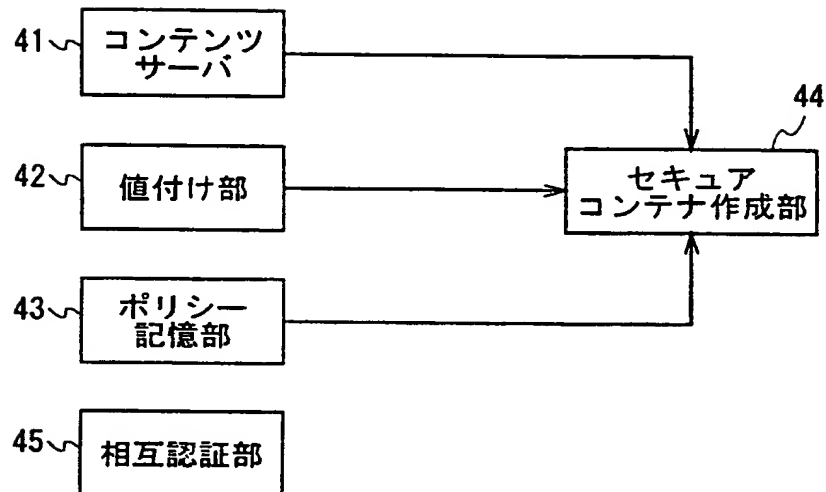


図 18



サービスプロバイダ 3-1

図 19

A	コンテンツのID		コンテンツAのID	
	コンテンツAのID		コンテンツAのID	
	UCPのID		UCPのID	
	PTのID		PTA-1のID	
	PTの有効期限		PTA-1の有効期限	
	価格条件 10		ユーザ条件 10	男性
			機器条件 10	条件なし
	価格内容 11		2000円	
	価格内容 12		600円	
	価格内容 13		100円	
	価格内容 14		300円	
B	コンテンツのID		コンテンツAのID	
	コンテンツAのID		コンテンツAのID	
	UCPのID		UCPのID	
	PTのID		PTA-2のID	
	PTの有効期限		PTA-2の有効期限	
	価格条件 20		ユーザ条件 20	女性
			機器条件 20	条件なし
	価格内容 21		1000円	
	価格内容 22		300円	
	価格内容 23		50円	
	価格内容 24		150円	

PTA-1

PTA-2

図 20

A

ユーザ条件 10	サービスコード	ハッシュコード	コンディションコード
	01 × × h	000000h	01h
機器条件 10	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1の価格条件 10

B

ユーザ条件 20	サービスコード	ハッシュコード	コンディションコード
	01 × × h	000001h	01h
機器条件 20	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2の価格条件 20

図 2 1

コンテンツのID	コンテンツAのID
コンテンツIDのID	コンテンツIDのID
UCPのID	UCPのID
サーバIDのID	サーバIDのID
PIのID	PIB-2のID
PIの有効期限	PIB-2の有効期限
価格条件 40	ユーザ条件 40 条件なし
価格内容 41	機器条件 40 主機器
価格内容 42	50円
	150円

PIB-2

B

コンテンツのID	コンテンツAのID
コンテンツIDのID	コンテンツIDのID
UCPのID	UCPのID
サーバIDのID	サーバIDのID
PIのID	PIB-1のID
PIの有効期限	PIB-1の有効期限
価格条件 30	ユーザ条件 30 条件なし
価格内容 31	機器条件 30 従機器
価格内容 32	100円
	300円

PIB-1

A

図 2 2

A

ユーザ条件 30	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	ハッシュコード	コンディションコード
	00××h	000064h	03h

PTB-1の価格条件 30

B

ユーザ条件 40	サービスコード	ハッシュコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	ハッシュコード	コンディションコード
	00××h	000064h	06h

PTB-2の価格条件 40

図 2 3

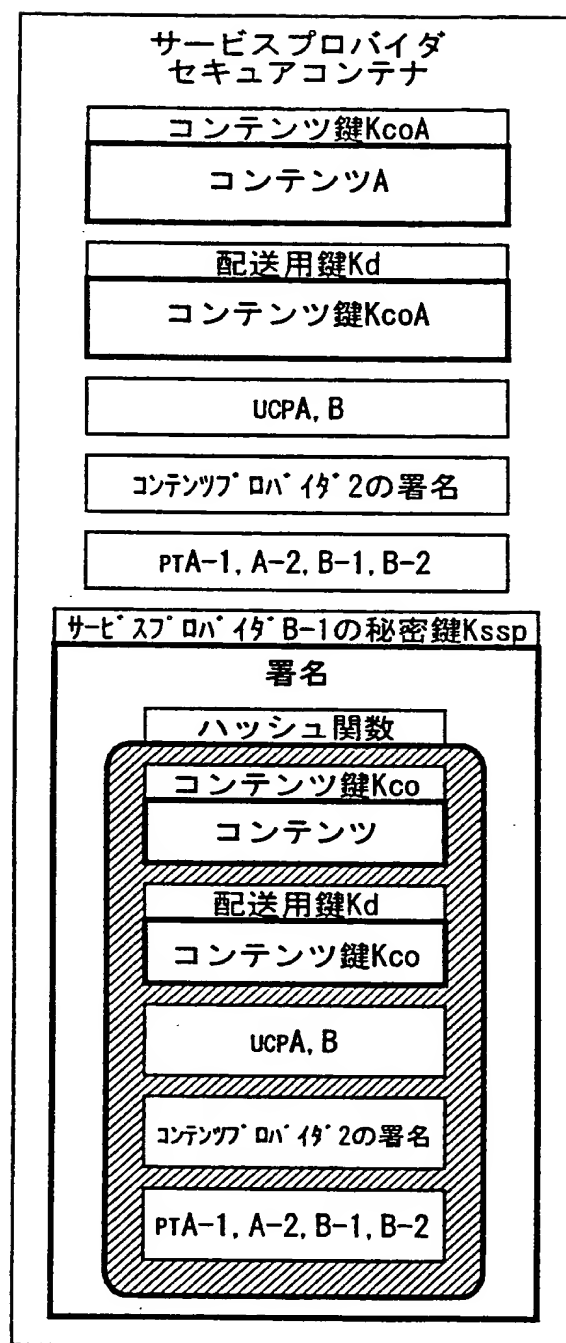


図 2 4

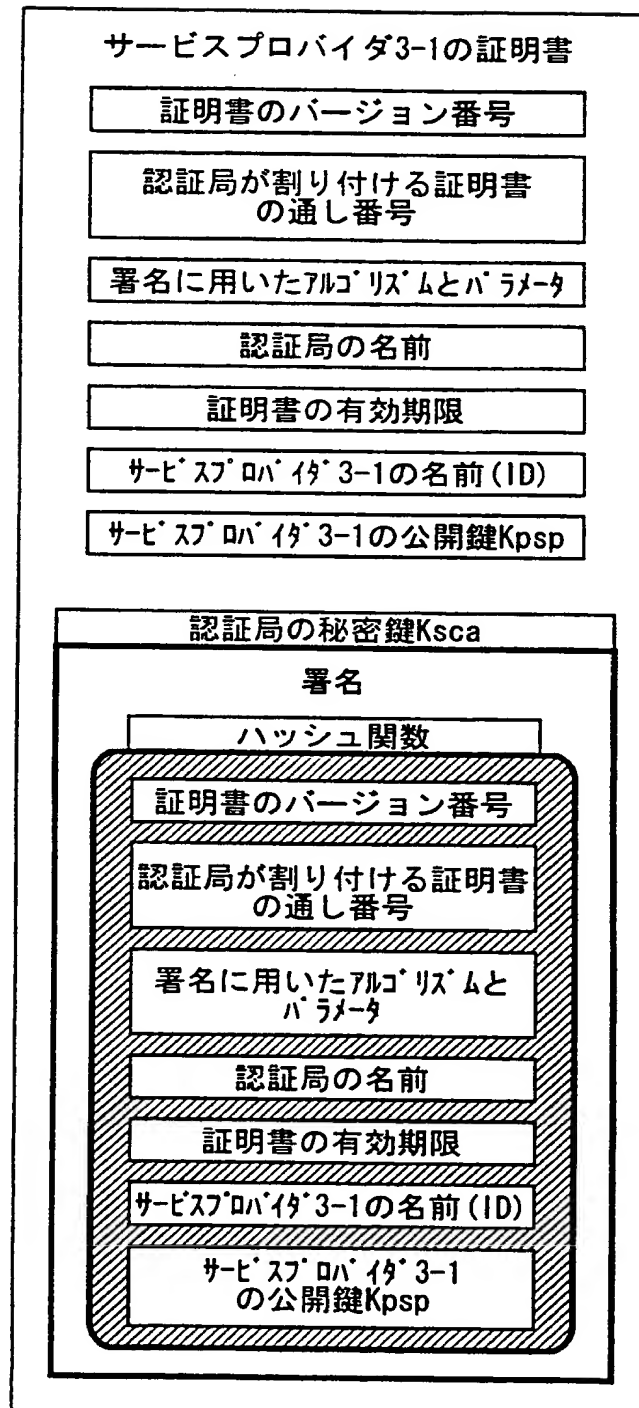


図 2 5

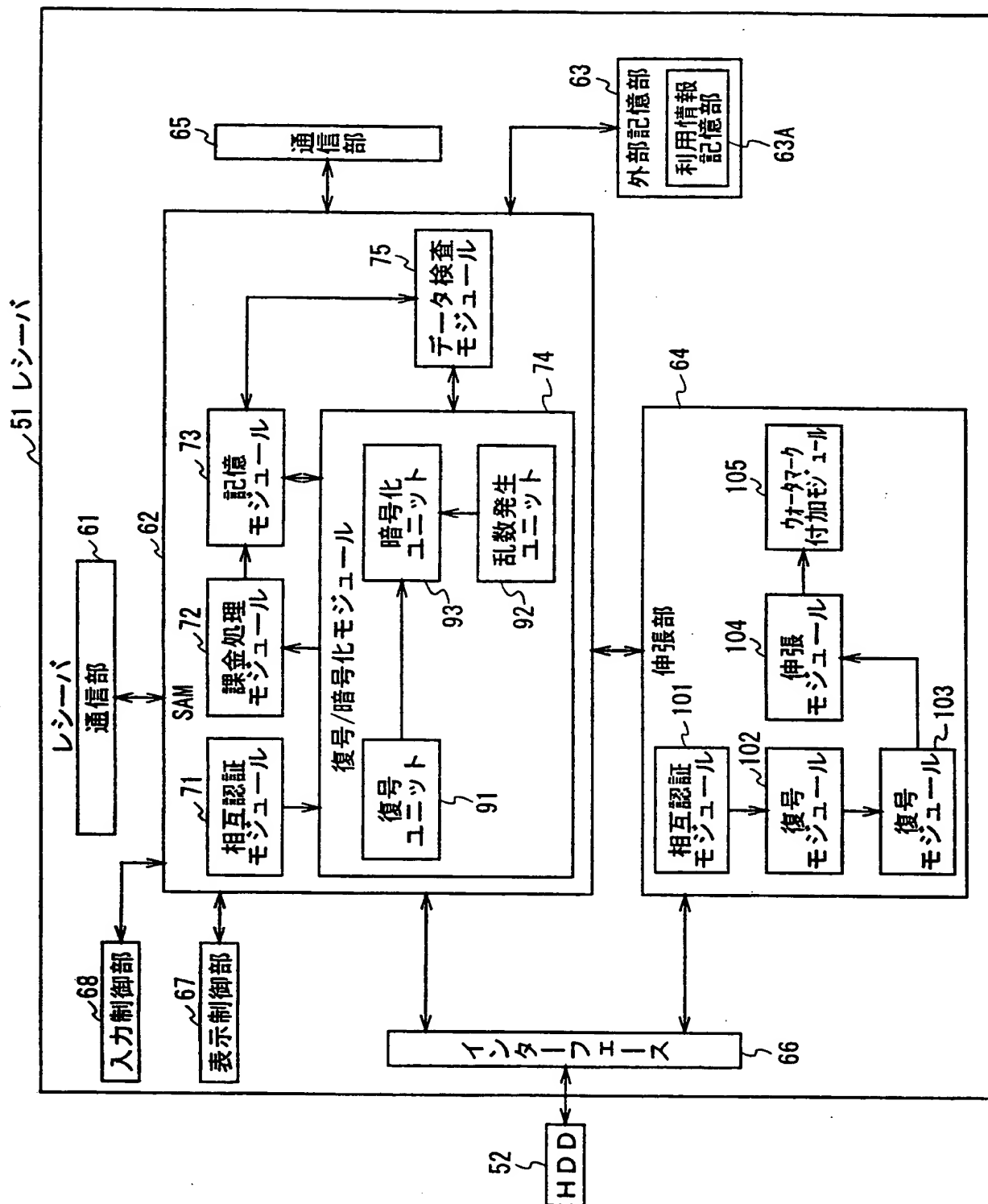


図 26

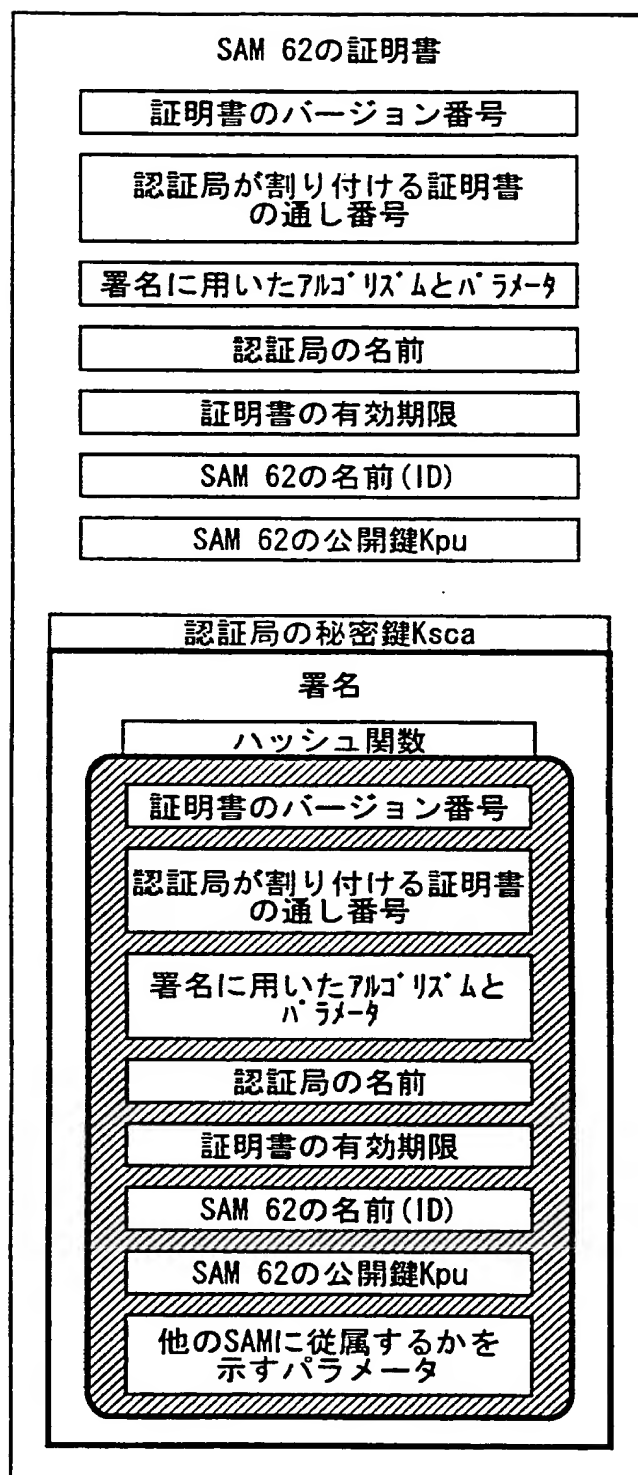


図 2 7

コンテンツのID		コンテンツAのID
コンテンツのID		コンテンツ 2-1のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスのID		サービス 3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容 11のID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
利用履歴		× × ×

ucsA

図 2 8

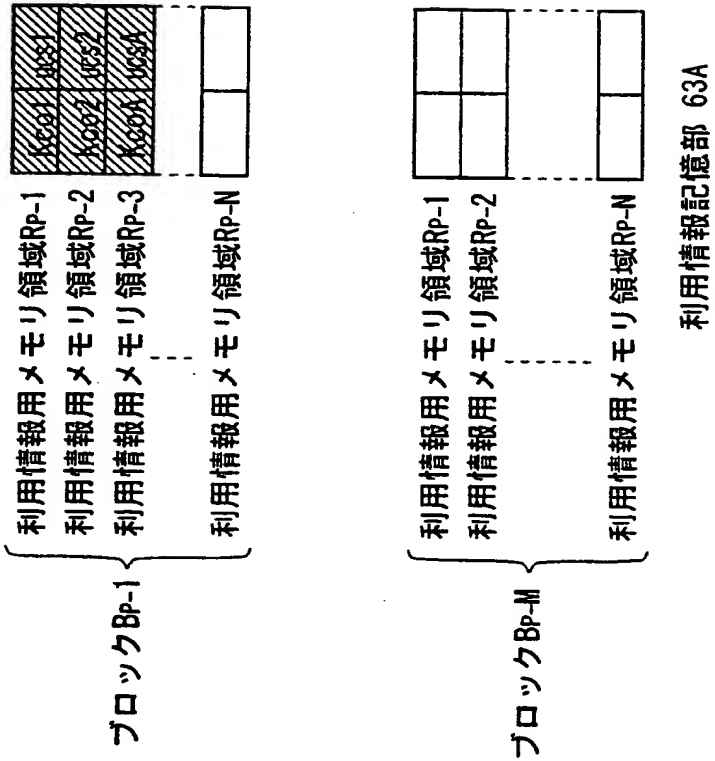


図 2 9

コンテンツのID		コンテンツAのID
コンテンツ「ロバ イダ」のID		コンテンツ「ロバ イダ」2-1のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービス「ロバ イダ」のID		サービス「ロバ イダ」3-1のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容11のID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62の ID、 管理移動先: SAM62の ID
課金履歴		× × ×

課金情報 A

図 3 0

SAM62の公開鍵Kpu		
SAM62の秘密鍵Ksu		
EMDサービスセンタ1の公開鍵Kpesc		
認証局の公開鍵Kpca		
保存用鍵Ksave		
3月分の配送用鍵Kd		
⋮		
SAM62証明書		
基準情報 51		
課金情報		
⋮		
検査値Hp-1	検査値Hp-2
.....		検査値Hp-M

図 3 1

SAMのID		SAM62のID
機器番号		レシーバ 51の機器番号 (100番)
決済ID		ユーザFの決済ID
課金の上限額		正式登録時の 課金の上限額
決済ユーザ情報	氏名	ユーザFの氏名
	住所	ユーザFの住所
	電話番号	ユーザFの電話番号
	決済機関情報	ユーザFの決済機関情報
	生年月日	ユーザFの生年月日
	年齢	ユーザFの年齢(21才)
	性別	ユーザFの性別(男)
	ユーザのID	ユーザFのID
	パスワード	ユーザFのパスワード
従属ユーザ情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザのID	
	パスワード	
利用ポイント情報		レシーバ 51の利用 ポイント情報

基準情報 51

図 3 2

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ 2-1	222ポイント
	コンテンツプロバイダ 2-2	123ポイント
	サービスプロバイダ 3-1	345ポイント
	サービスプロバイダ 3-2	0ポイント

基準情報51の利用ポイント情報

図 3 3

リスト部

SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
SAM62のID	ユーザFのID	可	可	SAM62のID	なし	制限なし	xxxx	xxxx

ユーザ51の登録条件

対象SAM ID
有効期限
バージョン番号
接続されている機器数

SAM62のID

xxxx

xxxx

1

対象SAM情報部

図 3 4

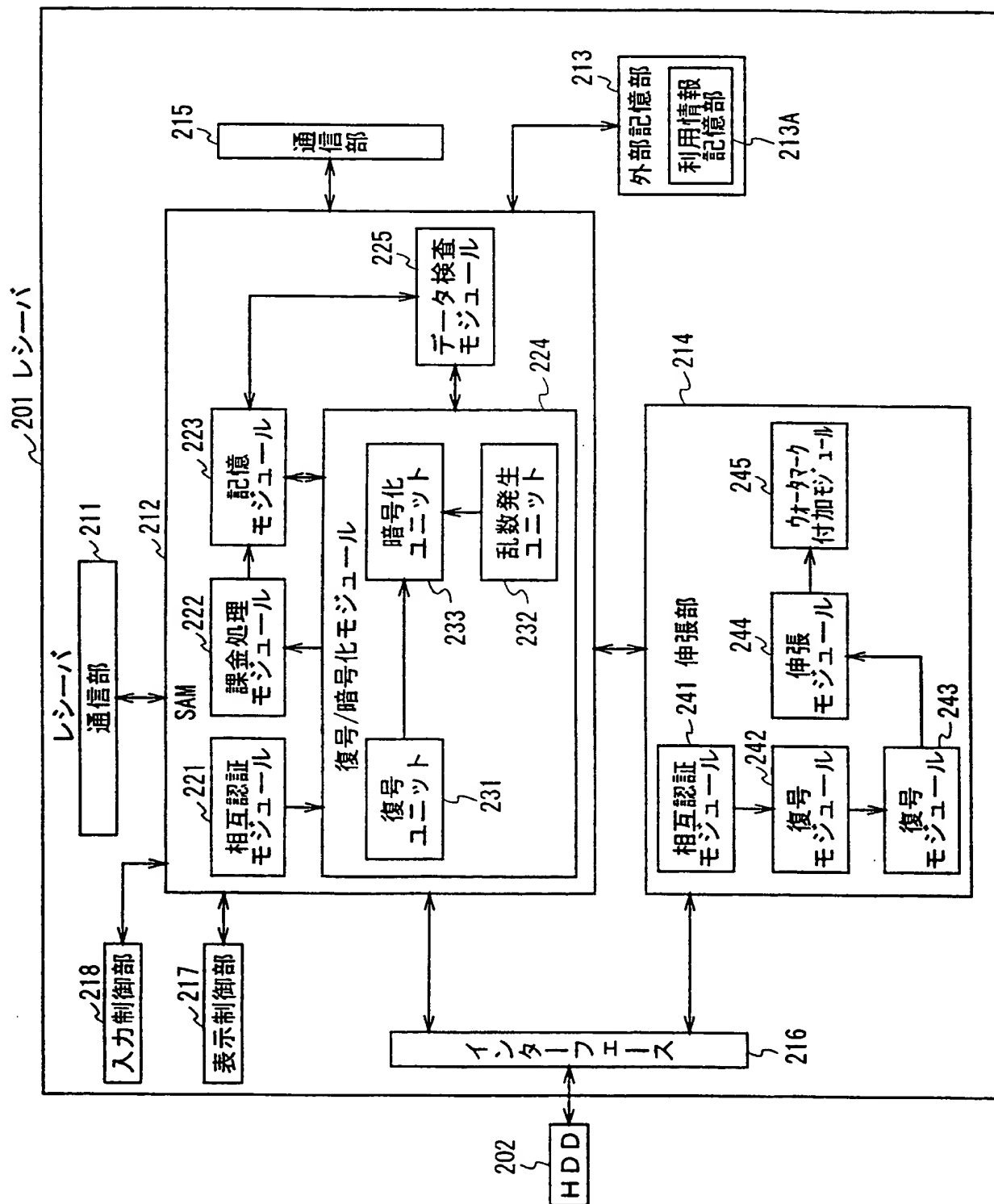


図35

SAM212の公開鍵Kpu		
SAM212の公開鍵Ksu		
EMDサービスセンタ1の公開鍵Kpesc		
認証局の公開鍵Kpca		
保存用鍵Ksave		
3月分の配送用鍵Kd		
⋮		
SAM212証明書		
基準情報 201		
⋮		
検査値Hp-1	検査値Hp-2
.....		検査値Hp-M

図 3 6

SAMのID		SAM62のID	
機器番号		レシバ 201の機器番号 (100番)	
決済ID		ユーザAの決済ID	
課金の上限額		正式登録時の 上限額	
決済 ユーザ 情報	氏名	ユーザAの氏名	
	住所	ユーザAの住所	
	電話番号	ユーザAの電話番号	
	決済機関情報	ユーザAの決済機関情報	
	生年月日	ユーザAの生年月日	
	年齢	ユーザAの年齢	
	性別	ユーザAの性別	
	ユーザのID	ユーザAのID	
	パスワード	ユーザAのパスワード	
従属 ユーザ 情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
⋮			
利用ポイント情報		レシバ 201の利用 ポイント情報	

基準情報 201

図 3 7

ユーザ	プロバイダ	利用ポイント
決済ユーザ	コンテンツプロバイダ2-1	23ポイント
	コンテンツプロバイダ2-2	22ポイント
	サービスプロバイダ3-1	40ポイント
	サービスプロバイダ3-2	5ポイント

基準情報201利用ポイント情報

図 3 8

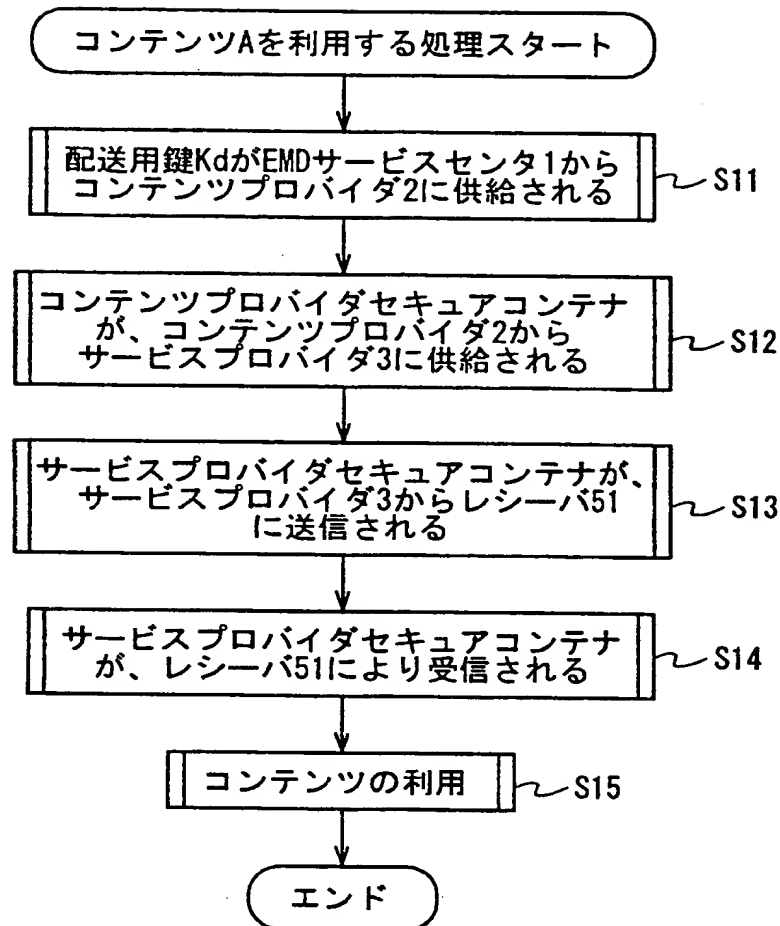


図 3 9

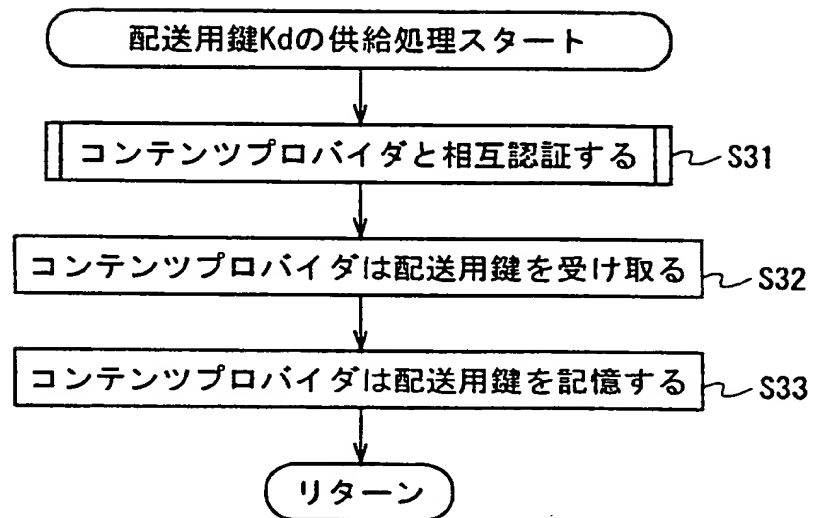


図 40

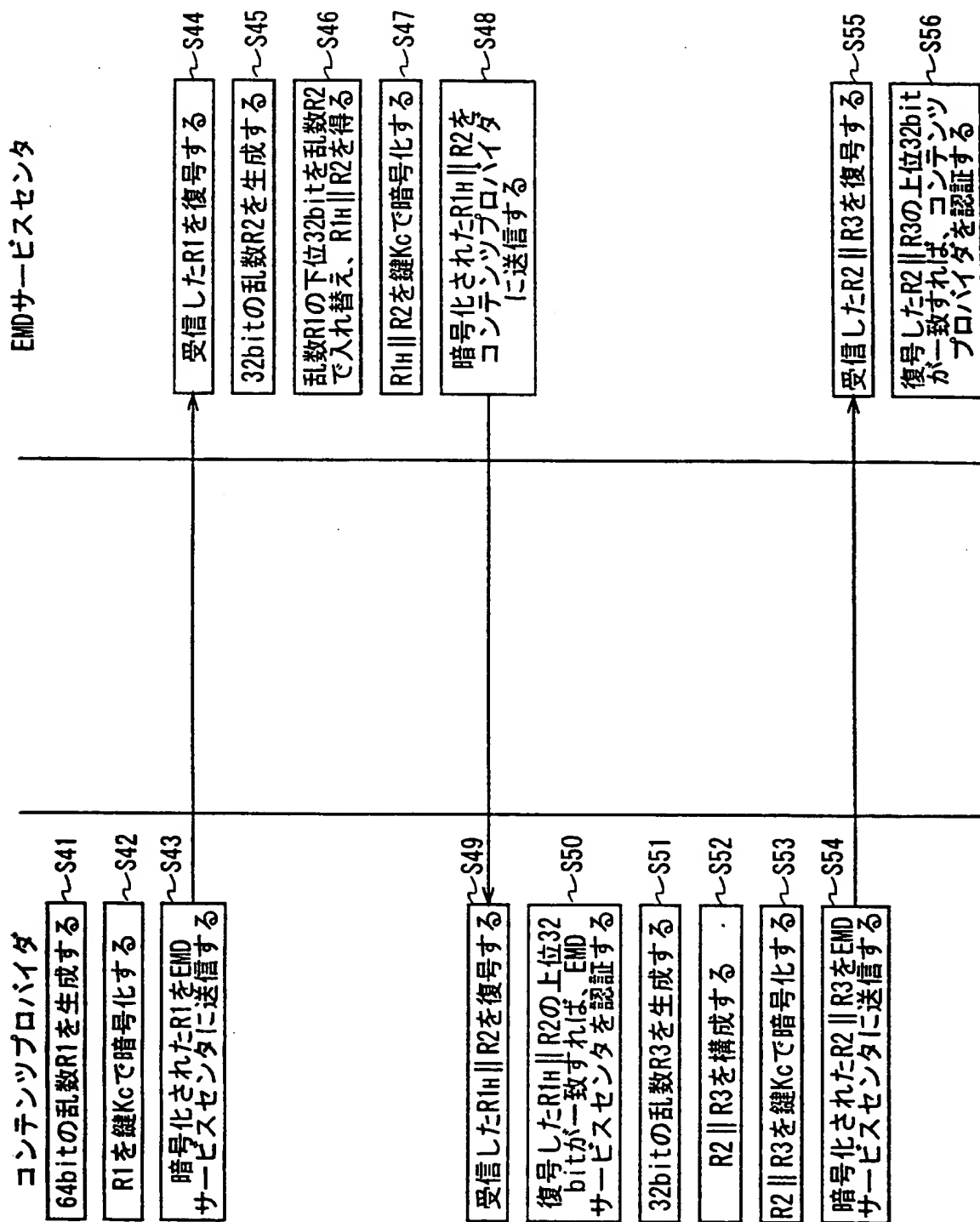


図 4 1

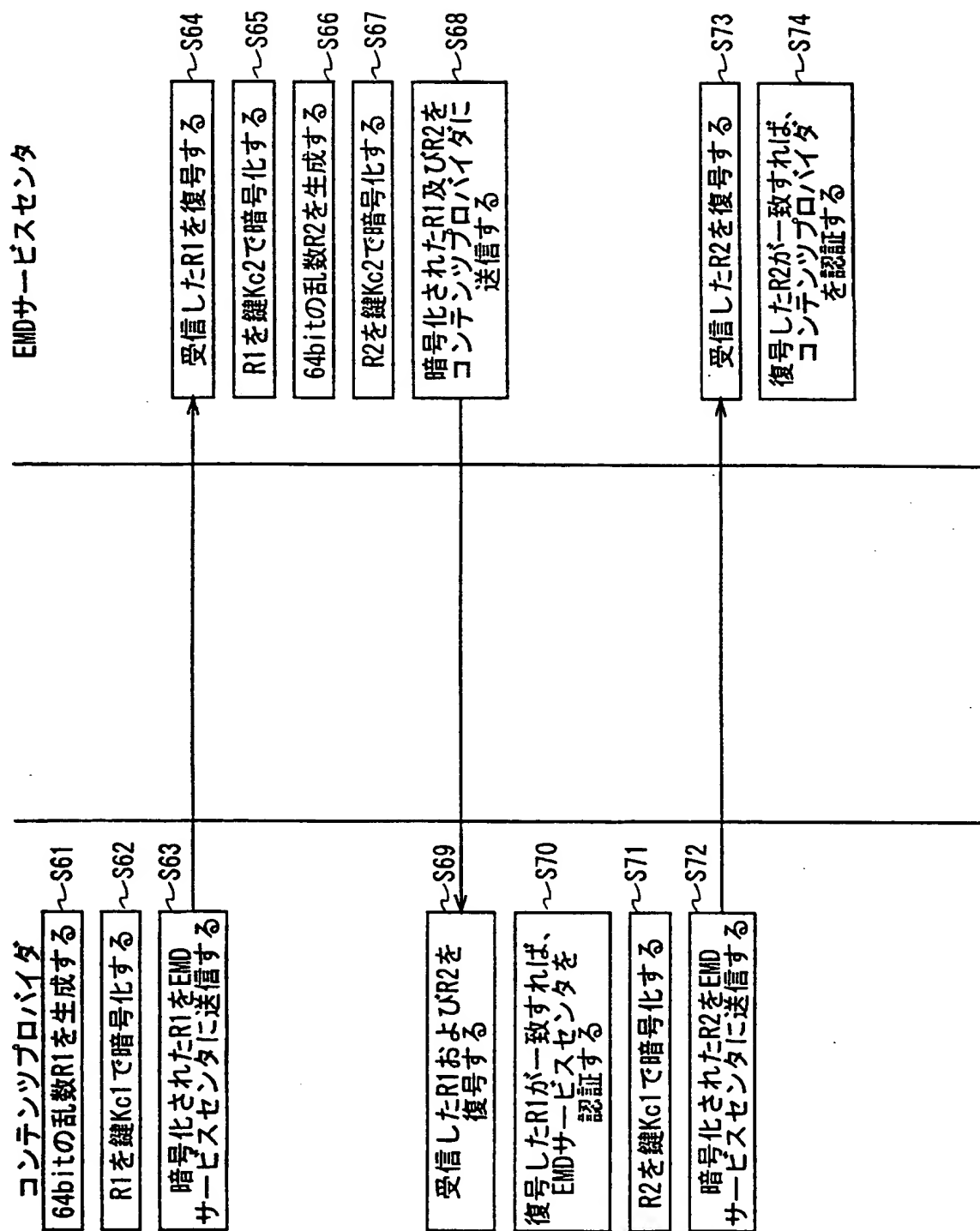


図 4 2

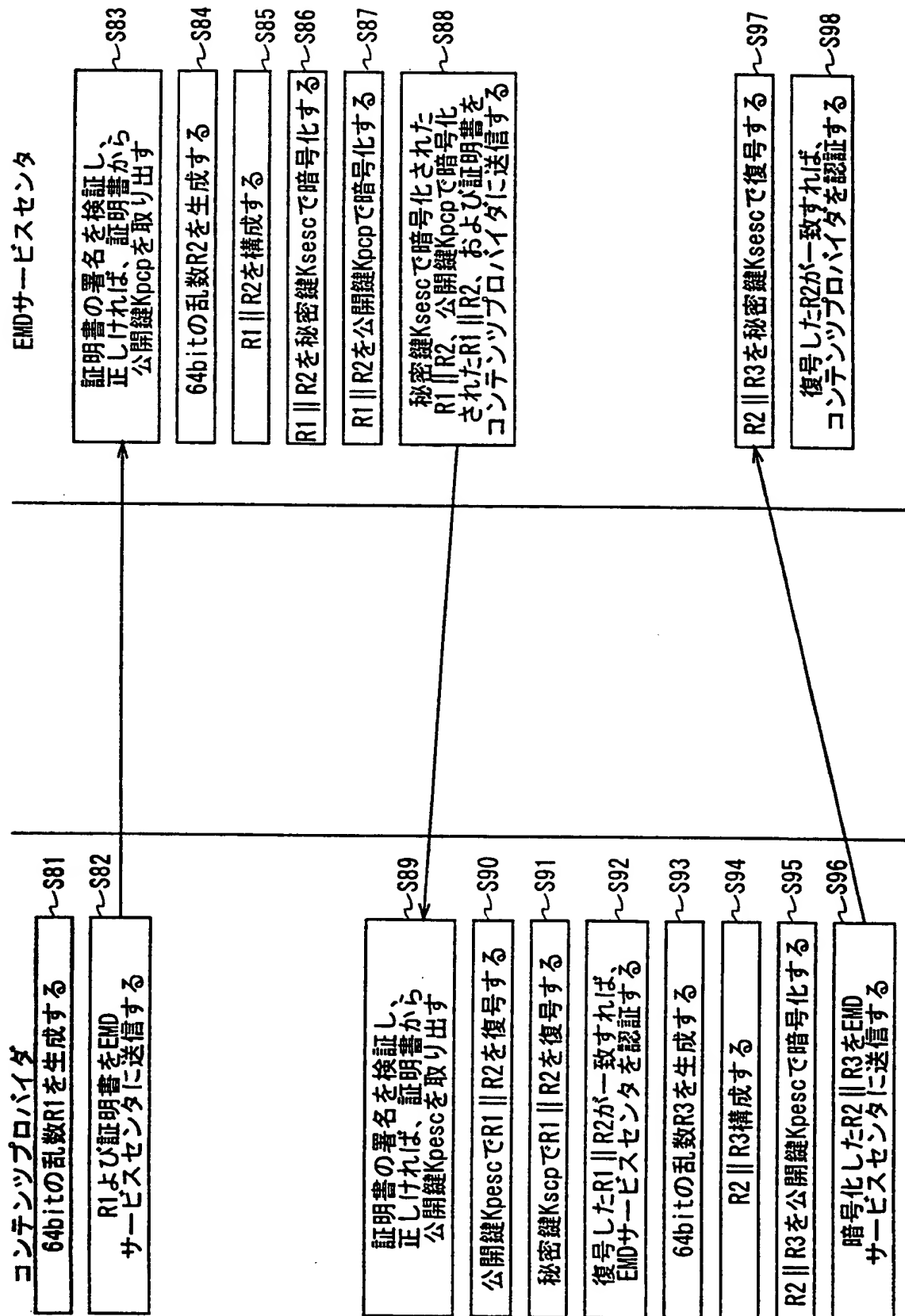


図 4 3

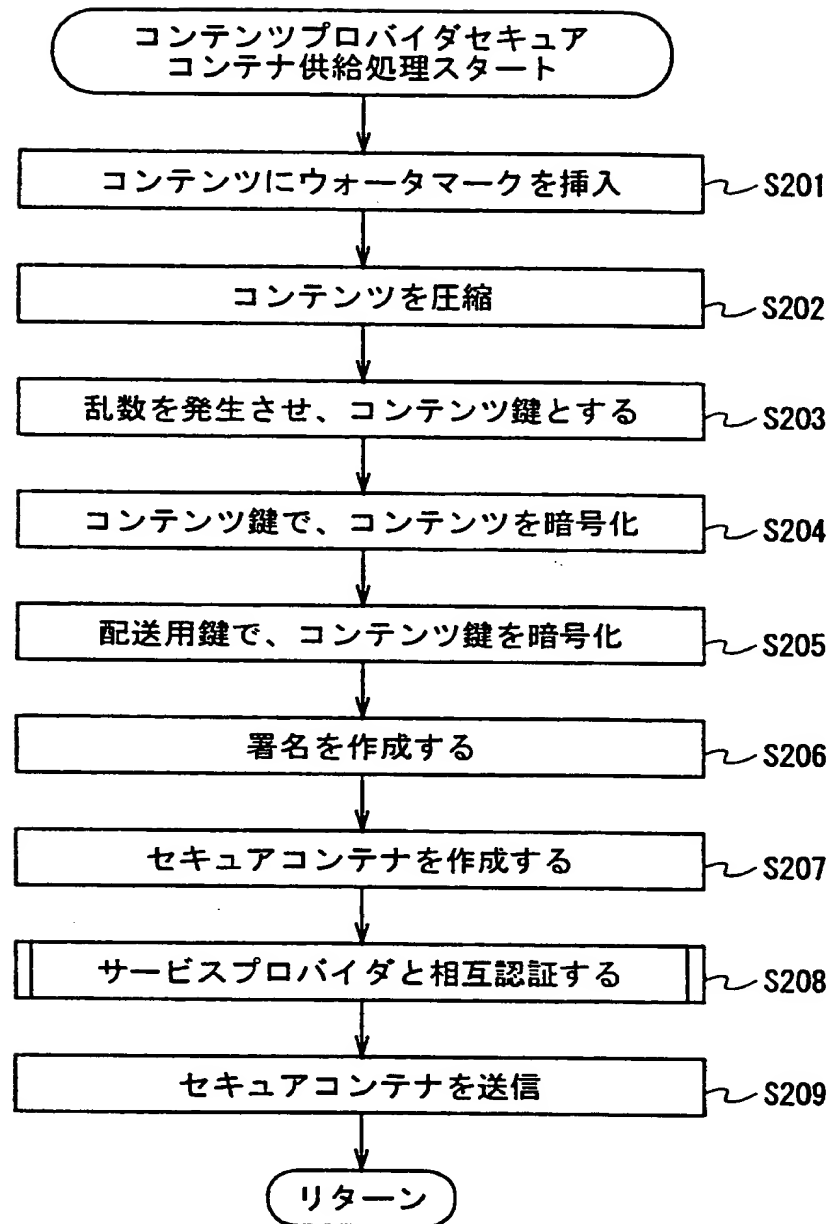


図 4 4

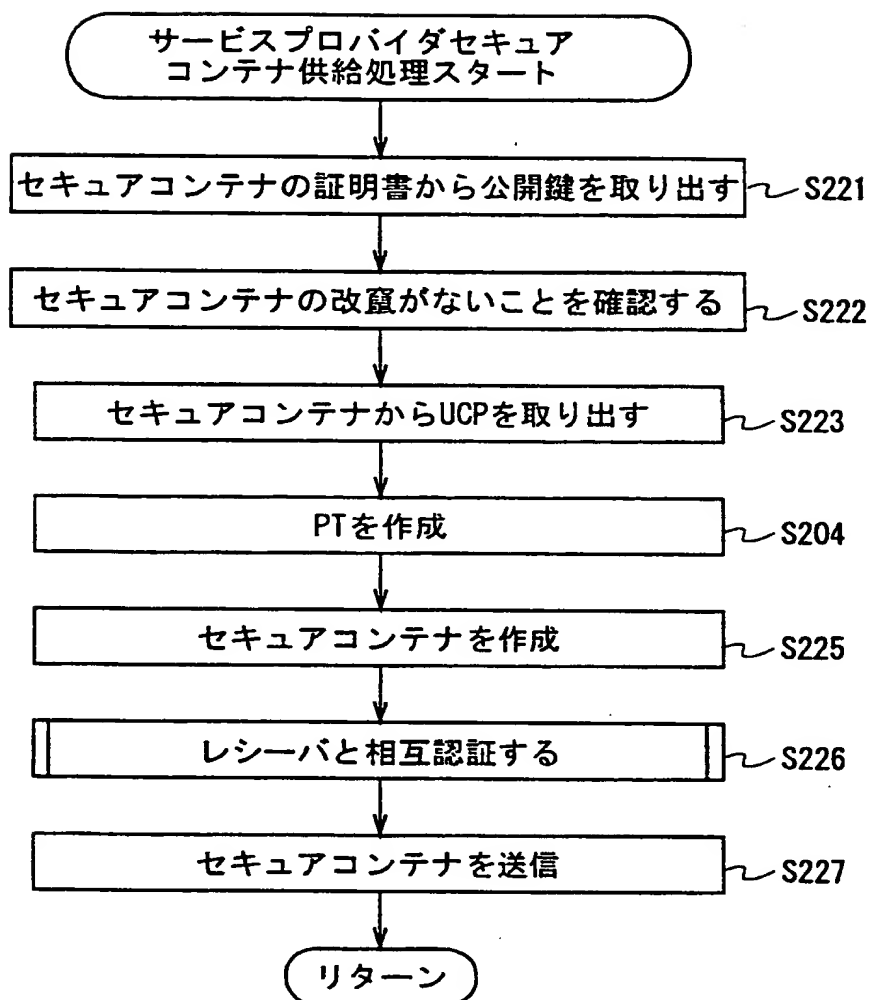


図 4 5

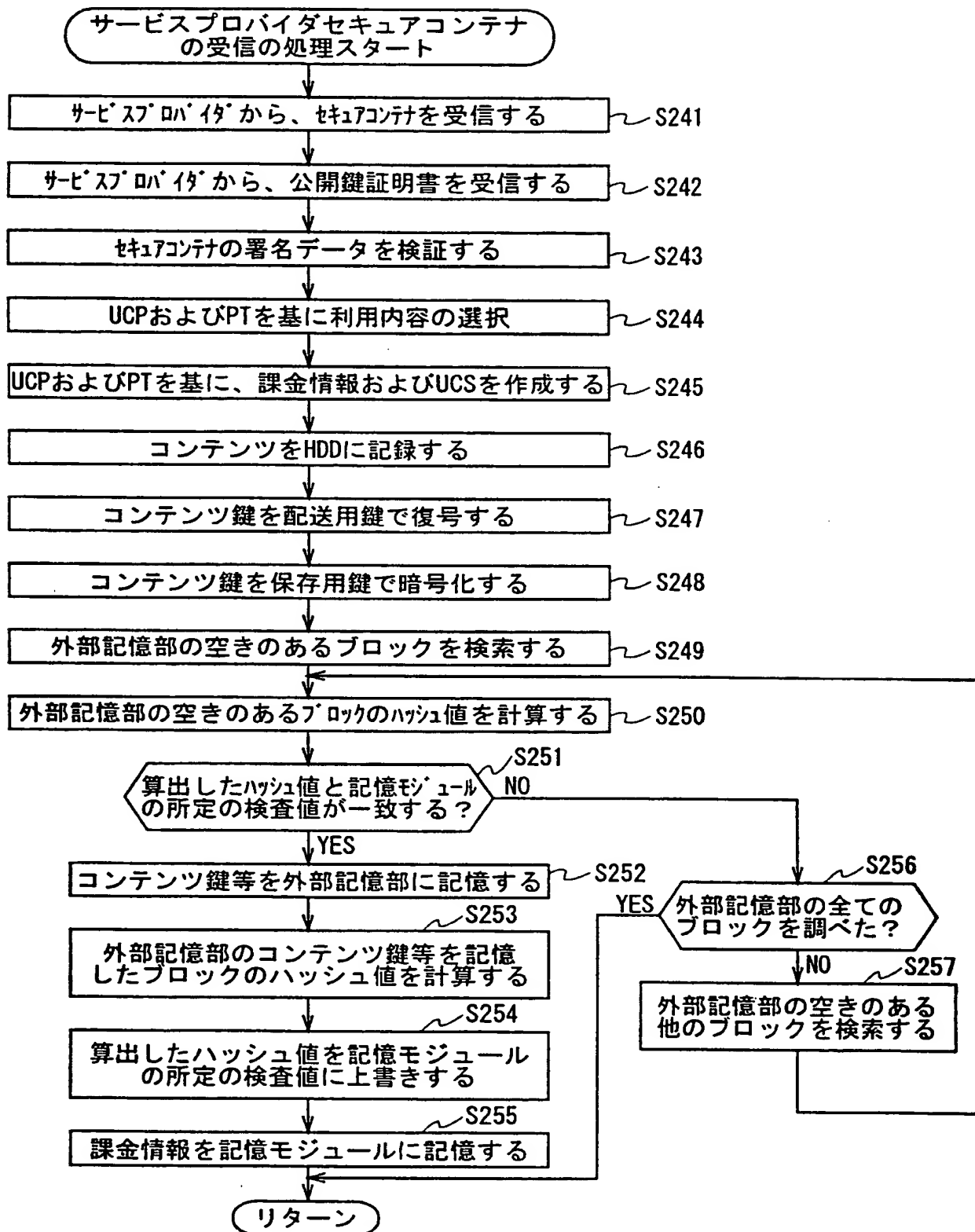


図 4 6

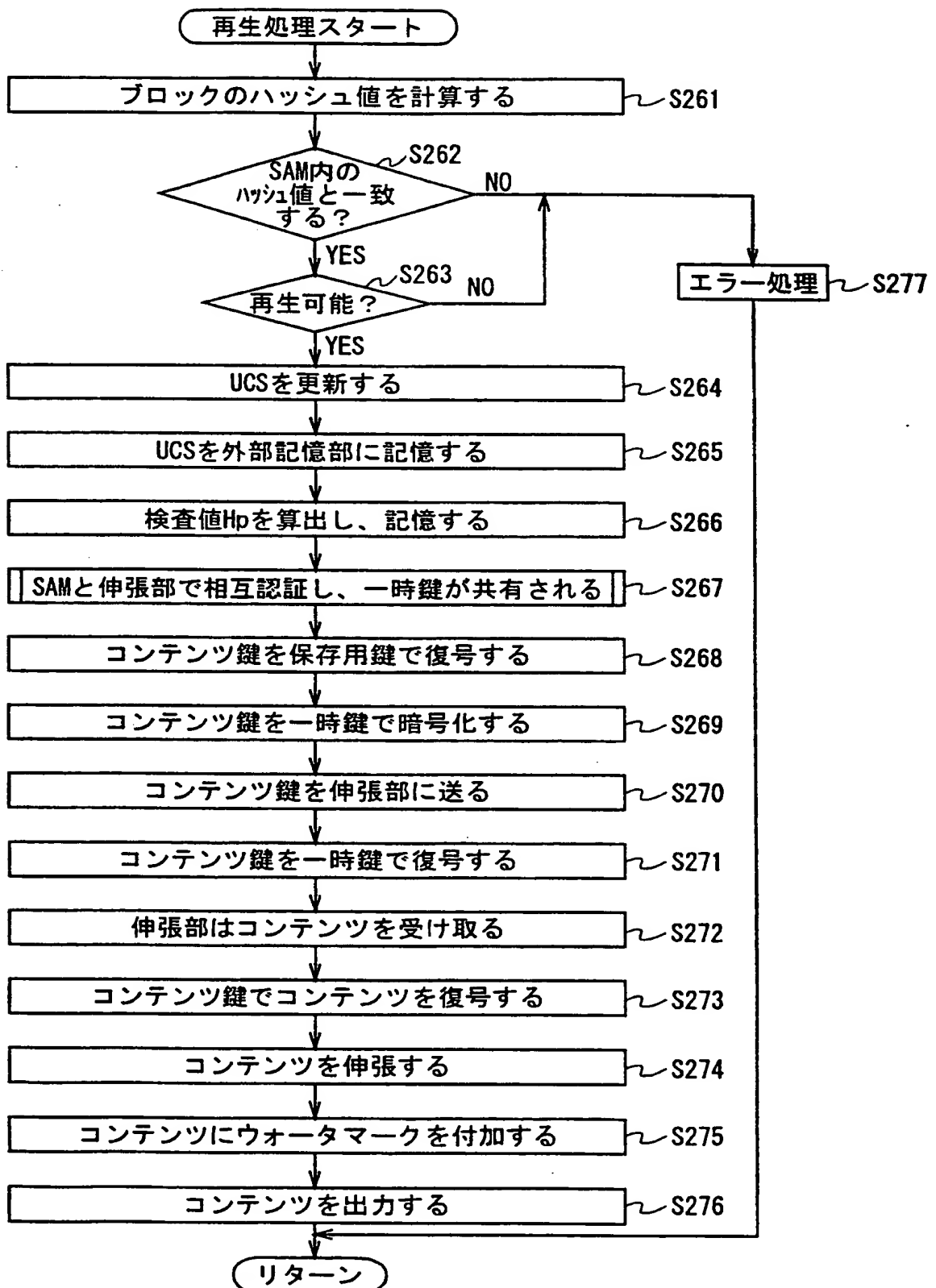


図 4 7

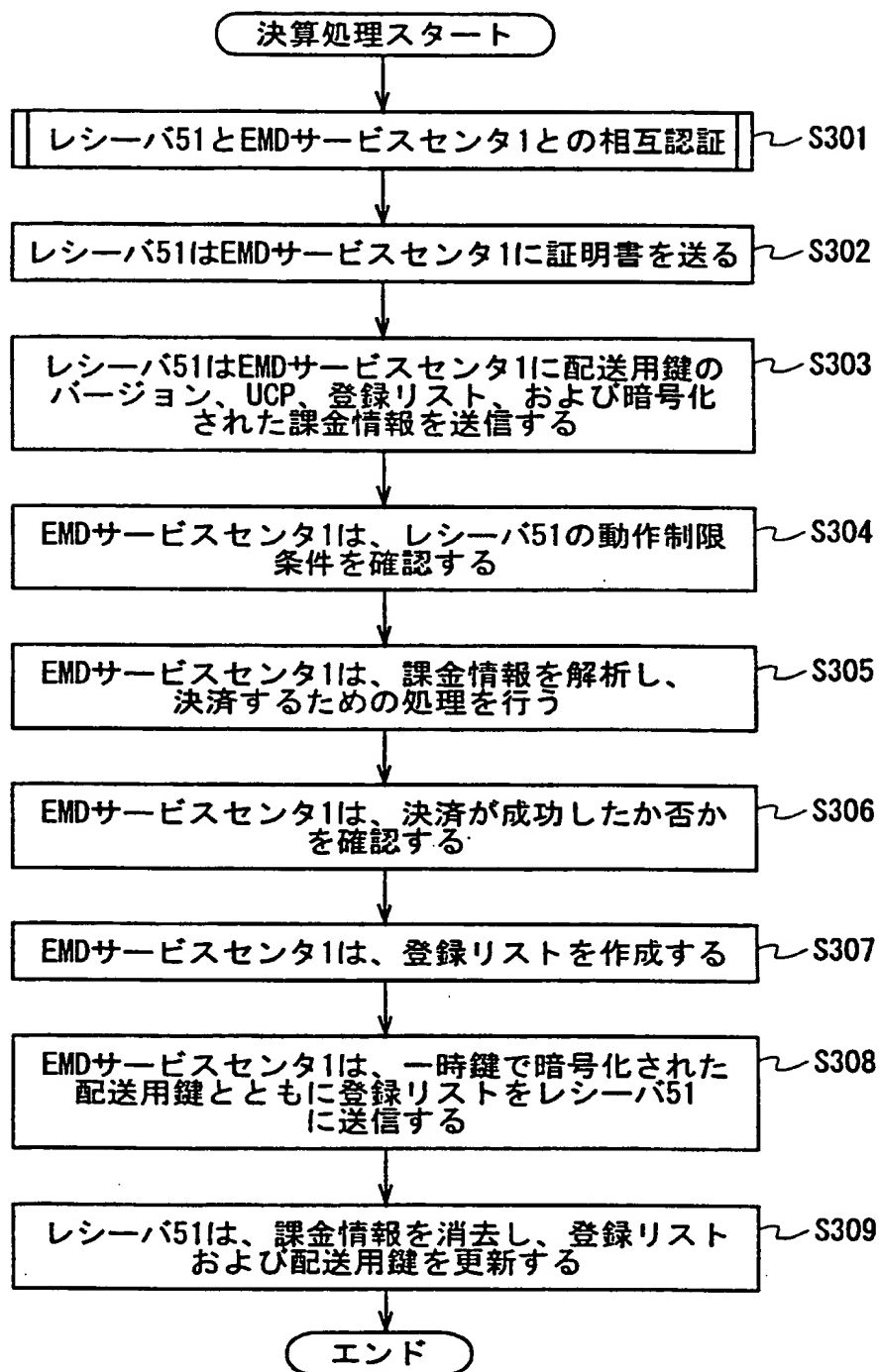


図 4 8

符 号 の 説 明

1... EMDサービスセンタ, 2... コンテンツプロバイダ, 3... サービスプロバイダ, 5... ユーザホームネットワーク, 11... サービスプロバイダ管理部, 12... コンテンツプロバイダ管理部, 13... 著作権管理部, 14... 鍵サーバ, 15... 経歴データ管理部, 16... 利益分配部, 17... 相互認証部, 18... ユーザ管理部, 19... 課金請求部, 20... 出納部, 21... 監査部, 31... コンテンツサーバ, 32... ウォータマーク付加部, 33... 圧縮部, 34... 暗号化部, 35... 乱数発生部, 36... 暗号化部, 37... ポリシー記憶部, 38... セキュアコンテナ作成部, 39... 相互認証部, 41... コンテンツサーバ, 42... 値付け部, 43... ポリシー記憶部, 44... セキュアコンテナ作成部, 45... 相互認証部, 51... レシーバ, 52... HDD, 61... 通信部, 62... SAM, 63... 外部記憶部, 64... 伸張部, 65... 信部, 66... インタフェース, 67... 表示制御部, 68... 入力制御部, 71... 相互認証モジュール, 72... 課金処理モジュール, 73... 記憶モジュール, 74... 復号/暗号化モジュール, 75... データ検査モジュール, 91... 復号ユニット, 92... 乱数発生ユニット, 93... 暗号化ユニット, 101... 相互認証モジュール, 102... 復号モジュール, 103... 復号モジュール, 104... 伸張モジュール, 105... ウォータマーク付加モジュール, 201... レシーバ, 202... HDD, 211... 通信部, 212... SAM, 213... 外部記憶部, 214... 伸張部, 215... 通信部, 216... インタフェース, 217... 表示制御部, 218... 入力制御部, 221... 相互認証モジュール, 222... 課金処理モジュール, 223... 記憶モジュール, 224... 復号/暗号化モジュール, 225... データ検査モジュール, 2

3 1... 復号ユニット, 2 3 2... 乱数発生ユニット, 2 3 3... 暗号化ユニット, 2 4 1... 相互認証モジュール, 2 4 2... 復号モジュール, 2 4 3... 復号モジュール, 2 4 4... 伸張モジュール, 2 4 5... ウォータマーク付加モジュール

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02289

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F17/60, G06F13/00, G09C1/00, H04L9/08, G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST Data Base (JOIS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/27155, A2 (InerTrust Technologies Corp.), 6 September, 1996 (06.09.96) &JP, 10-512074, A	1-9
A	US, 6002771, A (Sun Microsystems, Incorporated), 22 May, 1996 (22.05.96) & JP, 10-055383, A	1-9

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
24 May, 2000 (24.05.00)

Date of mailing of the international search report
13 June, 2000 (13.06.00)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

国際調査報告

国際出願番号 PCT/JP00/02289

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl¹ G06F17/60

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl¹ G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年
 日本国公開実用新案公報 1971-2000年
 日本国実用新案登録公報 1996-2000年
 日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTデータベース (JOIS)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO, 96/27155, A2 (InerTrust Technologies Corp.), 6. 9月. 1996 (06. 09. 96&JP, 10-512074, A	1-9
A	US, 6002771, A (Sun Microsystems, Incorporated) 22. 5月. 96 (22. 05. 96)&JP, 10-055383, A	1-9

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

24. 05. 00

国際調査報告の発送日

13.06.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
 郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

岩間 直純

5L

9287

電話番号 03-3581-1101 内線 3532